

NETOPIA® FIRMWARE USER GUIDE

3300-ENT ENTERPRISE SERIES

NETOPIA FIRMWARE VERSION 8.4



netopia®
BROADBAND WITHOUT BOUNDARIES™

Copyright

Copyright© 2004, Netopia, Inc. Netopia and the Netopia logo are registered trademarks belonging to Netopia, Inc., registered U.S. Patent and Trademark Office. Broadband Without Boundaries and 3-D Reach are trademarks belonging to Netopia, Inc. All other trademarks are the property of their respective owners. All rights reserved.

Netopia, Inc.
6001 Shellmound Street
Emeryville, CA 94608
U.S.A.

Part Number

Netopia part number 6161196-00-01

Chapter 1 — Introduction.....	1-1
What's New in 8.4	1-1
Telnet-based Management.....	1-2
Netopia Telnet Menus	1-2
Netopia Models	1-3
Screen differences	1-3
Connecting through a Telnet Session.....	1-3
Configuring Telnet software	1-4
Navigating through the Telnet Screens.....	1-4
Chapter 2 — WAN and System Configuration	2-1
WAN Configuration	2-1
WAN Ethernet Configuration screen	2-2
ADSL Line Configuration screen	2-4
Creating a New Connection Profile.....	2-9
Advanced Connection Options.....	2-14
Configuration Changes Reset WAN Connection	2-14
Scheduled Connections.....	2-15
Backup Configuration	2-20
Priority Queuing (TOS bit).....	2-20
System Configuration Screens	2-22
System configuration features.....	2-22
IP Setup.....	2-23
Filter Sets	2-23
IP Address Serving.....	2-23
Network Address Translation (NAT)	2-23
Stateful Inspection.....	2-23
Date and time	2-29
Wireless configuration	2-30
SNMP (Simple Network Management Protocol).....	2-36
Security.....	2-36
Upgrade Feature Set	2-36
Change Device to a Bridge.....	2-37

Logging	2-38
Chapter 3 — Multiple Network Address Translation	3-1
Overview	3-1
Features	3-2
Supported traffic	3-5
Support for AOL Instant Messenger (AIM) File Transfer	3-5
Support for Yahoo Messenger.....	3-6
MultiNAT Configuration	3-6
Easy Setup Profile configuration	3-6
Server Lists and Dynamic NAT configuration.....	3-7
IP setup	3-7
Modifying map lists.....	3-12
Adding Server Lists.....	3-15
Modifying server lists.....	3-17
Deleting a server	3-19
Binding Map Lists and Server Lists	3-21
IP profile parameters.....	3-21
IP Parameters (WAN Default Profile)	3-23
NAT Associations	3-25
IP Passthrough	3-27
MultiNAT Configuration Example	3-31
Chapter 4 — Virtual Private Networks (VPNs).....	4-1
Overview	4-1
About PPTP Tunnels	4-4
PPTP configuration	4-4
About IPsec Tunnels.....	4-7
About L2TP Tunnels	4-8
L2TP configuration	4-8
About GRE Tunnels	4-11
VPN force-all.....	4-14
About ATMP Tunnels.....	4-15

ATMP configuration	4-15
Encryption Support	4-17
MS-CHAP V2 and 128-bit strong encryption	4-18
ATMP/PPTP Default Profile.....	4-18
VPN QuickView	4-20
Dial-Up Networking for VPN.....	4-21
Installing Dial-Up Networking.....	4-21
Creating a new Dial-Up Networking profile	4-22
Configuring a Dial-Up Networking profile	4-23
Connecting using Dial-Up Networking.....	4-24
Allowing VPNs through a Firewall.....	4-24
PPTP example.....	4-26
ATMP example	4-28
Windows Networking Broadcasts.....	4-31
Chapter 5 — Internet Key Exchange (IKE) IPsec	
Key Management for VPNs	5-1
Overview	5-1
Internet Key Exchange (IKE) Configuration.....	5-2
Adding an IKE Phase 1 Profile	5-4
Changing an IKE Phase 1 Profile	5-7
Key Management.....	5-8
Advanced IPsec Options	5-11
IPsec WAN Configuration Screens	5-18
IPsec Manual Key Entry.....	5-19
VPN Quickview	5-20
WAN Event History Error Reporting.....	5-21
Chapter 6 — IP Setup	6-1
IP Setup.....	6-2
IP subnets.....	6-4
Static routes	6-6
RIP-2 MD5 Authentication.....	6-10
Overview	6-10

Authentication configuration.....	6-10
Connection Profiles and Default Profile	6-15
IP Address Serving	6-17
IP Address Pools.....	6-20
DHCP NetBIOS Options	6-21
More Address Serving Options.....	6-23
Configuring the IP Address Server options	6-24
DHCP Relay Agent.....	6-28
Connection Profiles	6-30
Multicast Forwarding.....	6-33
Chapter 7 — Line Backup	7-1
Configuring Backup	7-1
Connection Profiles	7-2
IP Setup.....	7-7
WAN Configuration	7-8
Backup Configuration screen	7-10
Using Scheduled Connections with Backup.....	7-12
Backup Default Gateway.....	7-14
Backup Configuration screen	7-14
IP Setup screen	7-16
Backup Management/Statistics.....	7-17
QuickView	7-18
Chapter 8 — Monitoring Tools	8-1
Quick View Status Overview.....	8-1
General status.....	8-2
Current status	8-3
Status lights.....	8-3
Statistics & Logs	8-4
Event Histories	8-4
IP Routing Table.....	8-7
General Statistics	8-7
System Information.....	8-9

Simple Network Management Protocol (SNMP).....	8-10
The SNMP Setup screen.....	8-11
SNMP traps.....	8-12
Chapter 9 — Security	9-1
Suggested Security Measures.....	9-1
Telnet Tiered Access – Two Password Levels	9-2
UPnP Support.....	9-2
Superuser configuration	9-3
Limited user configuration	9-4
Advanced Security Options	9-6
User access password	9-8
User menu differences.....	9-9
Telnet Access	9-16
About Filters and Filter Sets.....	9-17
What's a filter and what's a filter set?	9-17
How filter sets work	9-17
How individual filters work	9-18
Design guidelines	9-23
Working with IP Filters and Filter Sets	9-24
Adding a filter set.....	9-25
Deleting a filter set	9-29
A sample filter set.....	9-29
Policy-based Routing using Filtersets	9-32
TOS field matching.....	9-33
Firewall Tutorial	9-35
General firewall terms	9-35
Basic IP packet components.....	9-35
Basic protocol types.....	9-35
Firewall design rules	9-36
Filter basics.....	9-38
Example filters.....	9-39
Configuration Management	9-42

TFTP	9-44
Chapter 10 — Utilities and Diagnostics	10-1
Ping	10-2
Trace Route	10-4
Telnet Client	10-5
Factory Defaults	10-6
Transferring Configuration and Firmware Files with TFTP..	10-6
Updating firmware	10-7
Downloading configuration files	10-7
Uploading configuration files	10-8
Restarting the System	10-8
Appendix A — Troubleshooting.....	A-1
Configuration Problems	A-1
Network problems.....	A-2
How to Reset the Router to Factory Defaults.....	A-3
Power Outages	A-3
Technical Support.....	A-3
How to reach us	A-4
Appendix B — Understanding IP Addressing	B-1
What is IP?.....	B-1
About IP Addressing	B-1
Subnets and subnet masks	B-2
Example: Using subnets on a Class C IP internet ...	B-3
Example: Working with a Class C subnet.....	B-5
Distributing IP Addresses	B-5
Technical note on subnet masking	B-6
Configuration	B-7
Manually distributing IP addresses	B-8
Using address serving.....	B-8
Tips and rules for distributing IP addresses	B-9
Nested IP Subnets	B-11

Broadcasts.....	B-14
Packet header types	B-14
Appendix C — Binary Conversion Table.....	C-1
Appendix D — Technical Specifications and Safety Information ..	D-1
Description.....	D-1
Power requirements	D-1
Environment	D-1
Software and protocols	D-1
Agency approvals	D-2
North America	D-2
International.....	D-2
Manufacturer's Declaration of Conformance	D-3
Important Safety Instructions	D-4
FCC Part 68 Information.....	D-5
FCC Requirements	D-5
FCC Statements	D-5
Electrical Safety Advisory	D-7

Index

Chapter 1

Introduction

This *Firmware User Guide* covers the advanced features of the Netopia 3300-Series Router family.

Your Netopia equipment offers advanced configuration features accessed through the Main Menu of the Telnet configuration screen. This *Firmware User Guide* documents the advanced features, including advanced testing, security, monitoring, and configuration. This *Firmware User Guide* should be used as a companion to the *Quickstart Guide* and the *Getting Started Guide*. You should read the *Quickstart Guide* and the *Getting Started Guide* before reading this *Firmware User Guide*.

What's New in 8.4

New in Netopia Firmware Version 8.4 are the following features:

- IPSec MTU Support
See [“Advanced IPsec Options” on page 5-11](#).
- TACACS+ Support
See [“TACACS+ server authentication” on page 9-8](#).
- GRE Tunneling Support
See [“About GRE Tunnels” on page 4-11](#).
- Session Initiation Protocol ALG support setting in the CLI.

(The SIP ALG supports only SIP over UDP, not TCP.)

See the *Command Line Interface Commands Reference* available on the Netopia website.

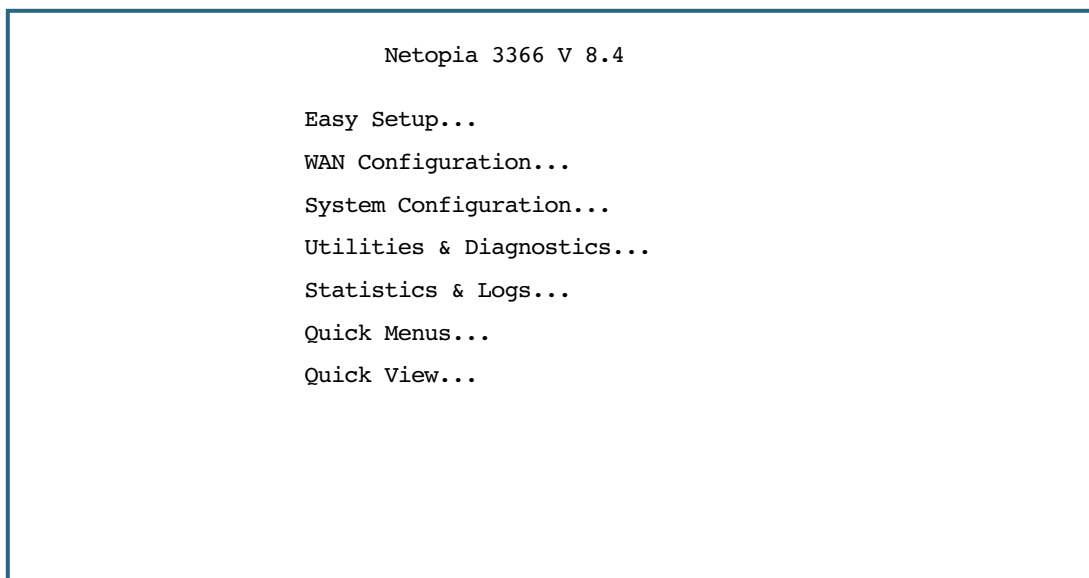
Telnet-based Management

Telnet-based management is a fast menu-driven interface for the capabilities built into the Netopia Firmware Version 8.4. Telnet-based management provides access to a wide variety of features that the Router supports. You can customize these features for your individual setup. This chapter describes how to access the Telnet-based management screens. This section covers the following topics:

- [“Netopia Telnet Menus” on page 1-2](#)
- [“Netopia Models” on page 1-3](#)
- [“Connecting through a Telnet Session” on page 1-3](#)
- [“Navigating through the Telnet Screens” on page 1-4](#)

Netopia Telnet Menus

Telnet-based management screens contain the main entry points to the Netopia Firmware Version 8.4 configuration and monitoring features. The entry points are displayed in the Main Menu shown below:



- The **Easy Setup** menu display and permit changing the values contained in the default connection profile. You can use Easy Setup to initially configure the Router directly through a Telnet session.

Easy Setup menus contain up to five descendant screens for viewing or altering these values. The number of screens depends on whether you have optional features installed.

The *Quickstart Guide* describes the Easy Setup menus to get you up and running quickly.
- The **WAN Configuration** menu displays and permits changing your connection profile(s), Virtual Private Networks (VPNs) and default profile, creating or deleting additional connection profiles, and configuring or reconfiguring the manner in which you may be using the Router to connect to more than one service

provider or remote site. See [“WAN Configuration,” beginning on page 2-1](#). See also [Chapter 4, “Virtual Private Networks \(VPNs\).”](#)

- The **System Configuration** menus display and permit changing:
 - IP Setup
 - IP Address Serving
 - Date and Time
 - Security
 - Change Device to a Bridge
 - Filter Sets
 - Network Address Translation (NAT)
 - SNMP (Simple Network Management Protocol)
 - Upgrade Feature Set
 - Logging

and more. See [“System Configuration Screens,” beginning on page 2-22](#).

- The **Utilities & Diagnostics** menus provide a selection of the various tools for monitoring and diagnosing the Router's behavior, as well as for updating the firmware and rebooting the system. See [Chapter 10, “Utilities and Diagnostics.”](#)
- The **Statistics & Logs** menus display several sets of tables and device logs that show information about your Router, your network, and their history. See [“Statistics & Logs,” beginning on page 8-4](#).
- The **Quick Menu** screen is a shortcut entry point to a variety of the most commonly used configuration menus that are accessed through the other menu entry points.
- The **Quick View** menu displays at a glance current real-time operating information about your Router. See [“Quick View Status Overview” on page 8-1](#).

Netopia Models

This *Firmware User Guide* covers all of the Netopia 3300-Series Router models. However some information in this guide will only apply to a specific model.

Screen differences

Because different Netopia 3300-Series models offer many different features and interfaces, the options shown on some screens in this *Firmware User Guide* may not appear on your own particular model's Telnet screen.

These differences are noted throughout the manual.

Connecting through a Telnet Session

Features of the Netopia Firmware Version 8.4 can be configured through the Telnet screens.

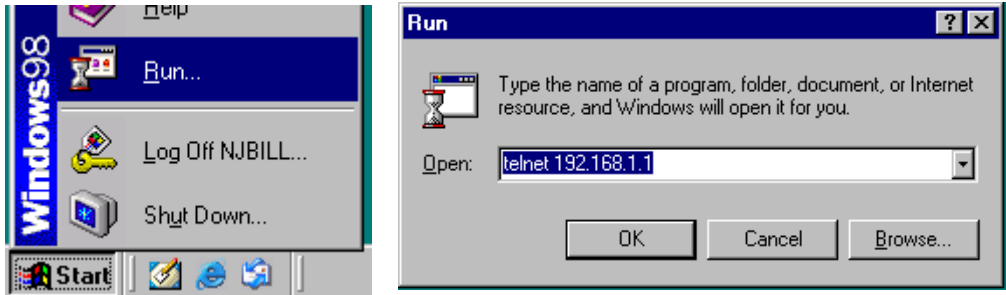
Before you can access the console screens through Telnet, you must have:

- A network connection locally to the Router or IP access to the Router.
- Telnet software installed on the computer you will use to configure the Router

Configuring Telnet software

If you are configuring your device using a Telnet session, your computer must be running a Telnet software program.

- If you connect a PC with Microsoft Windows, you can use a Windows Telnet application or run Telnet from the Start menu.



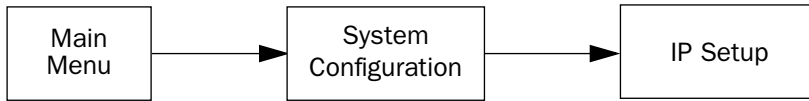
- If you connect a Macintosh computer running Classic Mac OS, you can use the NCSA Telnet program supplied on the Netopia CD. You install NCSA Telnet by dragging the application from the CD to your hard disk.
Mac OS X users can use the Terminal application that comes with Mac OS X in the Utilities folder.

Navigating through the Telnet Screens

Use your keyboard to navigate the Netopia Firmware Version 8.4’s configuration screens, enter and edit information, and make choices. The following table lists the keys to use to navigate through the Telnet screens.

To...	Use These Keys...
Move through selectable items in a screen or pop-up menu	Up, Down, Left, and Right Arrow
Set a change to a selected item or open a pop-up menu of options for a selected item like entering an upgrade key	Return or Enter
Change a toggle value (Yes/No, On/Off)	Tab
Restore an entry or toggle value to its previous value	Esc
Move one item up	Up arrow or Control + K
Move one item down	Down arrow or Control + O
Display a dump of the device event log	Control + E
Display a dump of the WAN event log	Control + F
Refresh the screen	Control + L

To help you find your way to particular screens, some sections in this guide begin with a graphical path guide similar to the following example:



This particular path guide shows how to get to the Network Protocols Setup screens. The path guide represents these steps:

1. Beginning in the Main Menu, select **System Configuration** and press Return. The System Configuration screen appears.
2. Select **IP Setup** and press Return. The IP Setup screen appears.

To go back in this sequence of screens, use the Escape key.

Chapter 2

WAN and System Configuration

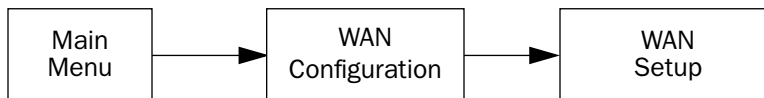
This chapter describes how to use the Telnet-based management screens to access and configure advanced features of your equipment. You can customize these features for your individual setup. These menus provide a powerful method for experienced users to set up their Router's connection profiles and system configuration.

This section covers the following topics:

- [“WAN Configuration” on page 2-1](#)
 - [“WAN Ethernet Configuration screen” on page 2-2](#)
 - [“ADSL Line Configuration screen” on page 2-4](#)
- [“Creating a New Connection Profile” on page 2-9](#)
- [“Advanced Connection Options” on page 2-14](#)
 - [“Configuration Changes Reset WAN Connection” on page 2-14](#)
 - [“Scheduled Connections” on page 2-15](#)
 - [“Backup Configuration” on page 2-20](#)
- [“System Configuration Screens” on page 2-22](#)
 - [“System configuration features” on page 2-22](#)

WAN Configuration

To configure your Wide Area Network (WAN) connection, navigate to the WAN Configuration screen from the Main Menu and select **WAN (Wide Area Network) Setup**.



The Line Configuration screen appears. The Line Configuration screen will be appropriate to the type of WAN interface supported by your particular Router model.

WAN Ethernet Configuration screen

The WAN Ethernet Configuration screen appears as follows:

WAN Ethernet Configuration

Address Translation Enabled:	Yes
Local WAN IP Address:	0.0.0.0
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
NAT Options...	
Stateful Inspection Enabled:	No
Filter Set...	
Remove Filter Set	
Enable PPP over Ethernet:	Off
WAN Ethernet Speed Setting...	Auto-Negotiation
Wan Ethernet MAC Address:	00:fc:de:fa:dd:02
DHCP Client Mode:	Standards-Based
RIP Options...	

Set up the basic IP attributes of your Ethernet Module in this screen.

- **Address Translation Enabled** allows you to specify whether or not the router performs Network Address Translation (NAT) on the Ethernet WAN port. NAT is enabled by default.
- **Local WAN IP Address** allows you to manually configure an IP address for use on the Ethernet WAN port. The value 0.0.0.0 indicates that the device will act as a DHCP client on the Ethernet WAN port and attempt to acquire an address from a DHCP server. By default, the router acts as a DHCP client on the Ethernet WAN port.
- The **Local WAN IP Mask** field becomes visible if you specify a Local WAN IP Address. This allows you to manually configure an IP subnet mask for use on the Ethernet WAN port. This item is visible only if you have configured a non-zero Ethernet IP Address; otherwise, the router obtains a subnet mask via DHCP.
- The **NAT Map List** and **NAT Server List** options are set to the defaults, **Easy-PAT List** and **Easy-Servers**. These provide standard NAT mappings. For more advanced NAT configurations, see [“Multiple Network Address Translation” on page 3-1](#).
- **NAT Options** allows you to specify IP Passthrough, allowing a single PC on the LAN to have the router’s public address assigned to it. See [“IP Passthrough” on page 3-27](#).
- If you set **Stateful Inspection Enabled** to **Yes**, you can enable a security feature for computers on your LAN when NAT is disabled. See [“Stateful Inspection” on page 2-23](#).
- The **Filter Set** pop-up allows you to associate an IP filter set with the Ethernet WAN port. See [“About Filters and Filter Sets” on page 9-17](#).
- **Remove Filter Set** allows you to remove a previously associated filter set.
- **Enable PPP over Ethernet** is **Off** by default. If your service provider uses PPPoE authentication toggle this to **On**.

- The **WAN Ethernet Speed Setting** is now configurable via a pop-up menu. Options are: Auto-Negotiation (the default), 100 Mbps Full Duplex, 100 Mbps Half Duplex, 10 Mbps Full Duplex, and 10 Mbps Half Duplex. This may be useful in mixed networks, where multiple routers have different ethernet speed capability. If you want to maintain a single speed setting for compatibility with multiple routers on your LAN, you can select a speed/duplex combination that all of your routers can match.
- The **Wan Ethernet MAC Address** is the hardware address of the Netopia device. Some service providers require a specific MAC address as part of their authentication process. In such a case, you can enter the MAC address that your service provider requires. If your service provider doesn't use this method, you don't need to change this field.
- The **DHCP Client Mode** setting depends on the type of access concentrator equipment your service provider uses. Most use **Standards-Based**. Alternatively, your provider may instruct you to select **Copper Mountain Specific**.
- The **RIP Options** selection displays the WAN Ethernet RIP Parameters screen.

WAN Ethernet RIP Parameters

Receive RIP:	Off
Transmit RIP:	v1
	v2
	Both

- The **Receive RIP** pop-up menu controls the reception and transmission of Routing Information Protocol (RIP) packets on the Ethernet WAN port. The default is Both.

The **Transmit RIP** pop-up menu is hidden if NAT is enabled.

Routing Information Protocol (RIP) is needed if there are IP routers on other segments of your Ethernet network that the Netopia Firmware Version 8.4 needs to recognize. Set to "Both" (the default) the Netopia Firmware Version 8.4 will accept information from either RIP v1 or v2 routers. Alternatively, select **Receive RIP** and select **v1** or **v2** from the popup menu. With Receive RIP set to "v1," the Netopia Router's Ethernet port will accept routing information provided by RIP packets from other routers that use the same subnet mask. Set to "v2," the Netopia Firmware Version 8.4 will accept routing information provided by RIP packets from other routers that use different subnet masks.

If you want the Netopia Router to advertise its routing table to other routers via RIP, select **Transmit RIP** and select **v1**, **v2 (broadcast)**, or **v2 (multicast)** from the popup menu. With Transmit RIP v1 selected, the Netopia Firmware Version 8.4 will generate RIP packets only to other RIP v1 routers. With Transmit RIP v2 (broadcast) selected, the Netopia Firmware Version 8.4 will generate RIP packets to all other hosts on the network. With Transmit RIP v2 (multicast) selected, the Netopia Firmware Version 8.4 will generate RIP packets only to other routers capable of recognizing RIP v2 packets.

ADSL Line Configuration screen

The ADSL Line Configuration screen is shown below:

ADSL Line Configuration

Circuit Type...	Multimode
Trellis Coding Enabled:	On
Signaling Mode...	FDM
Fast Retrain Enabled:	On
Wiring Type...	AutoSense
Data Link Encapsulation...	RFC1483

1. Select **Circuit Type** and from the pop-up menu choose the type of circuit to which you will be connecting: Multimode, T1.413, G.dmt, or G.lite.
2. Select **Trellis Coding Enabled**. Toggle it to On (the default) or Off.
3. Select **Signaling Mode** and choose Echo Cancellation or FDM (the default).
4. If you selected Multimode Circuit Type, the **Fast Retrain Enabled** field appears. Toggle it to On (the default) or Off.
5. The **Wiring Type** pop-up menu allows you to choose the type of copper pair wiring in use at your location. Usually, the default AutoSense will detect the type and adjust itself accordingly. If you want to set it yourself, and you know the type of wiring you have, choose either Tip/Ring (Inner Pair) or A/A1 (Outer Pair) from the pop-up menu.
6. Select **Data Link Encapsulation** and press Return. The pop-up menu will offer you the choice of PPP or RFC1483.

ATM Circuit Configuration

On ADSL WAN interfaces, the Asynchronous Transfer Mode (ATM) connection between the router and the central office equipment (DSLAM) is divided logically into one or more virtual circuits (VCs). A virtual circuit may be either a permanent virtual circuit (PVC) or a switched virtual circuit (SVC). Netopia Routers support PVCs.

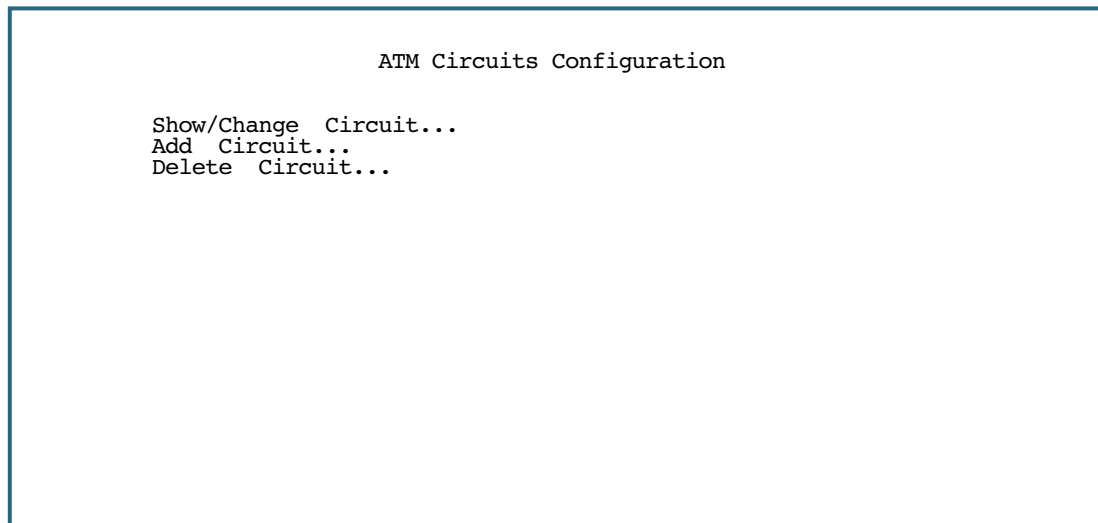
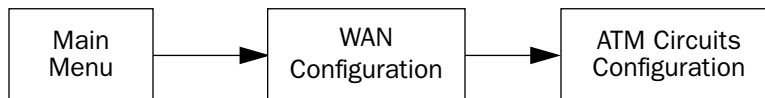
VCs are identified by a Virtual Path Identifier (VPI) and Virtual Channel Identifier (VCI). A VPI is an 8-bit value between 0 and 255, inclusive, while a VCI is a 16-bit value between 0 and 65535, inclusive.

- Circuits support attributes in addition to their VPI and VCI values. When configuring a circuit, you can specify an optional circuit name of up to 14 characters. The circuit name is used only to identify the circuit for management purposes as a convenience to aid in selecting circuits from lists. The default circuit name is “Circuit <n>”, where <n> is some number between one and eight corresponding to the circuit's position in the list of up to eight circuits.
- You can also individually enable or disable a circuit without deleting it. This is useful for temporarily removing a circuit without losing the configured attributes.
- In order to function, each circuit must be bound to a Connection Profile or to the Default Profile. Among other attributes, the profile binding specifies the IP addressing information for use on the circuit. Each circuit must be bound to a distinct Connection Profile.

ATM VPI/VCI Autodetection. You can bind multiple circuits to the same Connection Profile. Netopia Firmware Version 8.4 allows you to have a standard configuration that uses, for example, four VCs (0/35, 0/38, 8/35, 8/38) pointing to the same profile.

The unit will now automatically select the active VC on networks with a VPI/VCI of any of these four values without any custom configuration of the unit. You must, however, manually create these VCs and associate them with the profile you desire.

You configure Virtual Circuits in the Add/Change Circuit screen.



7. To add a circuit, select **Add Circuit** and press Return. The Add Circuit screen appears.

Add Circuit

Circuit Name:

Circuit 2

Circuit Enabled:

Yes

Circuit VPI (0-255):

0

Circuit VCI (32-65535):

QoS...

UBR

CBR

VBR

Peak Cell Rate (0 = line rate):

Use Connection Profile...

Default Profile

Use Default Profile for Circuit

ADD Circuit NOW

CANCEL

- Enter a name for the circuit in the Circuit Name field.
- Toggle **Circuit Enabled** to Yes.
- Enter the Virtual Path Identifier and the Virtual Channel Identifier in the **Circuit VPI** and **Circuit VCI** fields, respectively.
- The **Peak Cell Rate** field is editable. Netopia Firmware Version 8.4 supports three ATM classes of service for data connections: Unspecified Bit Rate (UBR), Constant Bit Rate (CBR), and Variable Bit Rate (VBR). You can configure these classes of service on a per VC basis. The default ATM class of service is UBR.

Quality of Service (QoS) settings

Note: QoS settings are not available on Ethernet-to-Ethernet WAN models.

- Select the **QoS** (Quality of Service) setting from the pop-up menu: **UBR**, **CBR**, or **VBR**.

UBR: No configuration is needed for UBR VCs. Leave the default value 0 (maximum line rate).
CBR: One parameter is required for CBR VCs. Enter the **Peak Cell Rate** that applies to the VC. This value should be between 1 and the line rate. You set this value according to specifications defined by your service provider.

Add Circuit	
Circuit Name:	Circuit 2
Circuit Enabled:	Yes
Circuit VPI (0-255):	0
Circuit VCI (32-65535):	32
QoS...	VBR
Peak Cell Rate (0 = line rate):	0
Sustained Cell Rate:	0
Maximum Burst Size:	0
Use Connection Profile...	Default Profile
Use Default Profile for Circuit	
ADD Circuit NOW	CANCEL

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.

VBR: This class is characterized by:

- a **Peak Cell Rate** (PCR), which is a temporary burst, not a sustained rate, and
- a **Sustained Cell Rate** (SCR),
- a Burst Tolerance (BT), specified in terms of **Maximum Burst Size** (MBS). The MBS is the maximum number of cells that can be transmitted at the peak cell rate and should be less than, or equal to the Peak Cell Rate, which should be less than, or equal to the line rate.

VBR has two sub-classes:

a. VBR non-real-time (VBR-nrt): Typical applications are non-real-time traffic, such as IP data traffic. This class yields a fair amount of Cell Delay Variation (CDV).

b. VBR real time (VBR-rt): Typical applications are real-time traffic, such as compressed voice over IP and video conferencing. This class transmits cells with a more tightly bounded Cell Delay Variation. The applications follow CBR.

- Then, select a Connection Profile for the Circuit. To use the Default Profile, select **Use Default Profile for Circuit** and press Return. For other options, select a profile from the **Use Connection Profile** pop-up menu.

Note: With multiple VCs you must explicitly statically bind the *second* (and all subsequent) VCs to a profile. The first VC will automatically statically bind according to pre-defined dynamic binding rules when you add the second VC. It will revert back to dynamic binding if the number of VCs is reduced to one; for example, by deleting previously defined VCs.

When the link comes up the router binds the VC dynamically to the first suitable Connection Profile or to the Default Profile if there is no Connection Profile configured.

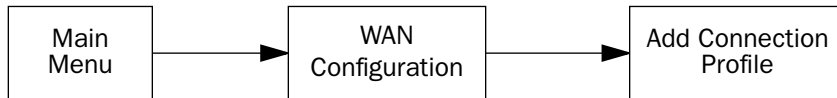
- If you factory default the router, the VC binds to the Default Profile.
- If you delete a Connection Profile that is statically bound to a VC, the VC binding is set back to the Default Profile. If there is only one VC defined, the VC dynamically binds to the first suitable profile or to the Default Profile. If there are multiple VCs defined, it binds to the Default Profile.
- If you add a second VC, it is initialized to the Default Profile, and the menu screens display the VC Connection Profile-related items, allowing you to bind to a specific Connection Profile instead of the Default Profile. In addition, the router statically binds the first VC according to the rules used to select a profile for dynamic binding. At this point, each profile uses static binding when the link is brought up.
- If there are no VCs when you add a VC – for example, if you deleted all your previous VCs and started adding them again – dynamic binding will occur when the link comes up. If you delete a VC, leaving only one VC, that VC resumes dynamically binding again.

-
- Select **ADD Circuit NOW** and press Return.
8. To display or change a circuit, select **Display/Change Circuit**, select a circuit from the pop-up menu, and press Return. The fields are the same as those in the Add Circuit screen.
 9. To delete a circuit, select Delete Circuit, select a circuit from the pop-up menu, and press Return. In the confirmation window, select CONTINUE and press Return.
 10. Press Escape to return to the WAN Setup menu.

Creating a New Connection Profile

Connection profiles are useful for configuring the connection and authentication settings for negotiating a PPP connection. If you are using the PPP data link encapsulation method, you can store your authentication information in the connection profile so that your user name and password (or host name and secret) are transmitted when you attempt to connect.

Connection profiles define the networking protocols necessary for the Router to make a remote connection. A connection profile is like an address book entry describing how the Router is to get to a remote site, or how to recognize and authenticate a connection. To create a new connection profile, you navigate to the WAN Configuration screen from the Main Menu, and select **Add Connection Profile**.



The **Add Connection Profile** screen appears.

Add Connection Profile

Profile Name:	Profile 1
Profile Enabled:	Yes
Encapsulation Type...	RFC1483
RFC1483 Mode...	Bridged 1483
IP Profile Parameters...	
<div style="display: inline-block; width: 45%;">COMMIT</div> <div style="display: inline-block; width: 45%;">CANCEL</div>	

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.
Configure a new Conn. Profile. Finished? COMMIT or CANCEL to exit.

On a Netopia Router you can add up to 15 more connection profiles, for a total of 16, but you can only use one at a time, unless you are using VPNs.

1. Select **Profile Name** and enter a name for this connection profile. It can be any name you wish. For example: the name of your ISP.
2. Toggle **Profile Enabled** to **Yes** or **No**. The default is Yes. You can toggle it to No, if you want to disable it later.
3. Select **Encapsulation Type** and press Return. The pop-up menu offers the possible data link encapsulation methods for connection profiles used for a variety of purposes: PPP, RFC1483, ATMP, PPTP, IPsec, or L2TP.

Multiple Data Link Encapsulation Settings

4. Select **Encapsulation Options** and press Return.
- If you selected ATMP, PPTP, L2TP, or IPSec, see [Chapter 4, “Virtual Private Networks \(VPNs\).”](#)
 - If you selected PPP or RFC1483, the screen offers different options:

Add Connection Profile

Profile Name:	Profile 1
Profile Enabled:	Yes
Encapsulation Type...	+-----+ +-----+ Bridged 1483 Routed 1483 +-----+
RFC1483 Mode...	
IP Profile Parameters...	
COMMIT	CANCEL

Add Connection Profile

Profile Name:	Profile 1
Profile Enabled:	Yes
Encapsulation Type...	PPP
Underlying Encapsulation...	None
PPP Mode...	VC Multiplexed
Encapsulation Options...	
IP Profile Parameters...	
Interface Group...	Primary
COMMIT	CANCEL

Configure a new Conn. Profile. Finished? COMMIT or CANCEL to exit.

- If you selected RFC1483, the screen allows you to choose **Bridged 1483** or **Routed 1483**.
- If you selected PPP, the screen allows you to choose **PPPoE** or **None** as the **Underlying Encapsulation**.
- If you choose **None**, the **PPP Mode** offers the choice of **VC Multiplexed** or **LLC SNAP**.

If you are using PPP, when you select **Encapsulation Options**, the Datalink (PPP/MP) Options screen appears. (RFC1483 does not require these options and does not offer the menu selection.)

Datalink (PPP/MP) Options

Data Compression...	Standard LZS
Send Authentication...	PAP
Send User Name:	
Send Password:	
Receive User Name:	
Receive Password:	

Datalink (PPP/MP) Options

Data Compression...	Standard LZS
Send Authentication...	PAP
Send User Name:	
Send Password:	
Receive User Name:	
Receive Password:	
Dial on Demand:	Yes

- **Data Compression** defaults to **Standard LZS**. You can select **Ascend LZS**, if you are connecting to compatible equipment, or **None** from the pull-down menu.
- The **Send Authentication** pull-down menu lets you select **PAP**, **CHAP**, or **None**.
- Selecting PAP or CHAP allows you to enter your authentication credentials for both *sending* and *receiving* connections.
PAP requires a **User Name** and **Password**;
CHAP requires a **Host Name** and **Secret**.
The screen changes to accommodate your selection.
- If you are creating a Backup profile (supported models only), and have selected Backup as the Interface Group in the previous screen, you can toggle **Dial on Demand** to Yes (the default) or No. See [“Line Backup” on page 7-1](#) for more information.

Return to the Add Connection Profile screen by pressing Escape.

5. Select **IP Profile Parameters** and press Return. The IP Profile Parameters screen appears.

IP Profile Parameters

Address Translation Enabled:

Yes

IP Addressing...

Numbered

NAT Map List...

Easy-PAT List

NAT Server List...

Easy-Servers

NAT Options...

Stateful Inspection Enabled:

No

Local WAN IP Address:

0.0.0.0

Local WAN IP Mask:

0.0.0.0

Filter Set...

Remove Filter Set

RIP Profile Options...

Return/Enter to select <among/between> ...

Configure IP requirements for a remote network connection here.

6. Toggle or enter your IP Parameters.

For more information, see:

- [“IP Setup” on page 6-2](#)
- [“Network Address Translation \(NAT\)” on page 2-23](#)
- [“Stateful Inspection Options” on page 2-24](#)
- [“Filter Sets” on page 2-23](#)
- The **RIP Profile Options** selection displays the RIP Profile Parameters screen.

RIP Profile Parameters

Receive RIP:

Off

v1

v2

Both v1 and v2

v2 MD5 Authentication

- The **Receive RIP** pop-up menu controls the reception and transmission of Routing Information Protocol (RIP) packets on the WAN port. The default is Both v1 and v2.
A **Transmit RIP** pop-up menu is hidden if NAT is enabled.
Routing Information Protocol (RIP) is needed if there are IP routers on other segments of your Ethernet network that the Netopia Router needs to recognize. Set to “Both” (the default) Netopia Firmware Version 8.4 will accept information from either RIP v1 or v2 routers. Alternatively, select **Receive RIP** and select **v1**, **v2**, or **v2 MD5 Authentication** from the popup menu. With Receive RIP set to “v1,” the Netopia Router’s Ethernet port will accept routing information provided by RIP packets from other routers that use the same subnet mask. Set to “v2,” the Netopia Firmware Version 8.4 will accept routing information provided by RIP packets from other routers that use different subnet masks.
For more information on v2 MD5 Authentication, see [“RIP-2 MD5 Authentication” on page 6-10](#).
- 7. Return to the Add Connection Profile screen by pressing Escape.
- 8. Select **COMMIT** and press Return. Your new Connection Profile will be added.
If you want to view the Connection Profiles in your device, return to the WAN Configuration screen, and select **Display/Change Connection Profile**. The list of Connection Profiles is displayed in a scrolling pop-up screen.

WAN Configuration	
+--Profile Name-----	IP Address-----+
Easy Setup Profile	255.225.255.255
Profile 1	0.0.0.0

You can also delete Connection Profiles by selecting them in the same manner using the **Delete Connection Profile** option in the WAN Configuration screen.

Advanced Connection Options

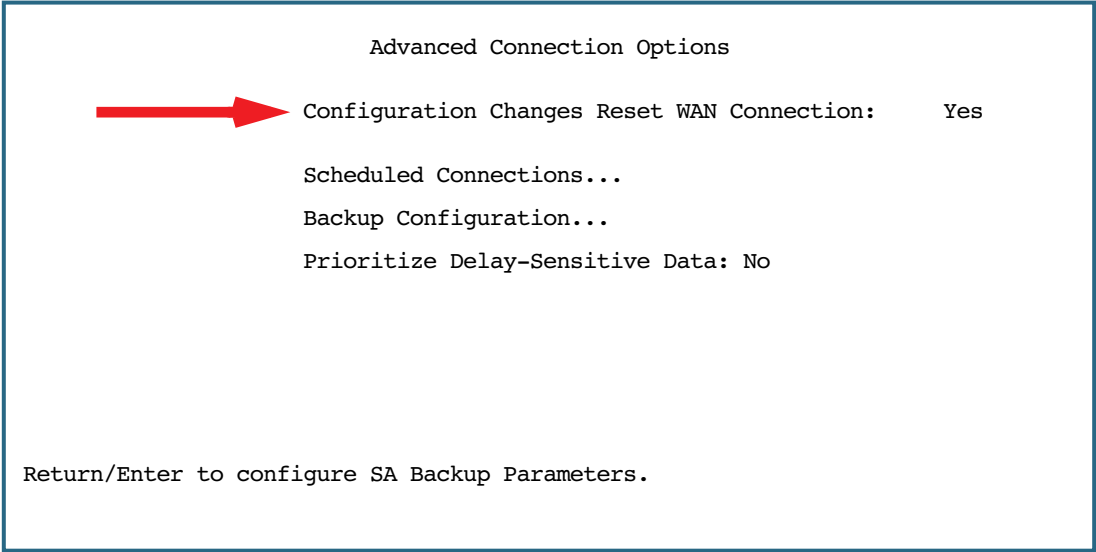
Configuration Changes Reset WAN Connection

The menu supports delaying some configuration changes until after the Netopia Router is restarted.

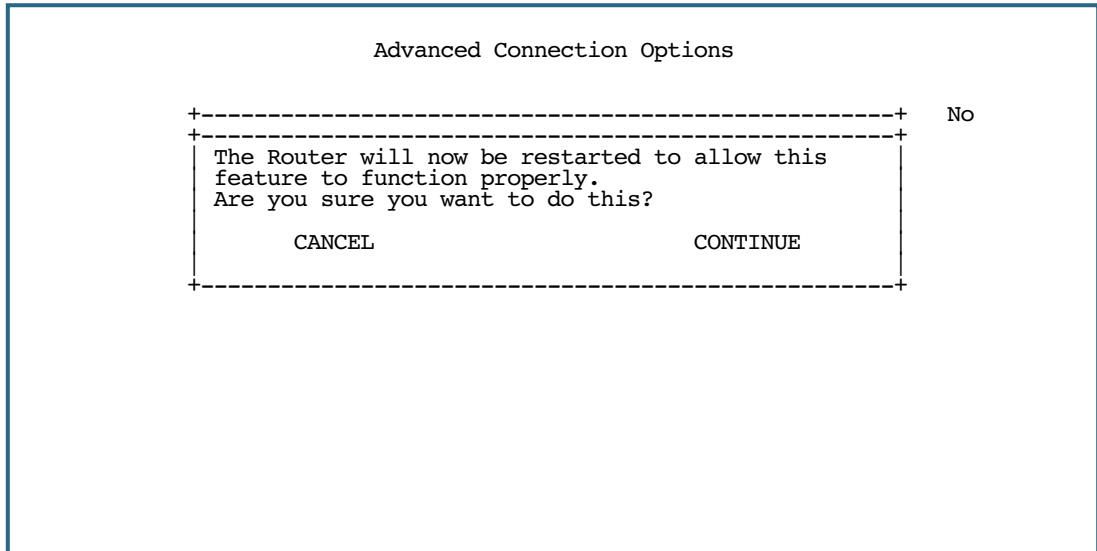
If your Netopia Router is preconfigured by your service provider, or if you are not remotely configuring the router, you can leave this setting unchanged.

The purpose of this feature is to defer configuration changes *only* when remotely configuring or reconfiguring the Netopia Router to prevent premature Telnet disconnection. When this feature is enabled, no changes to the WAN setup, datalink encapsulation, Connection Profiles, or Default Gateway will take effect until after the Netopia Router is restarted. Until the Netopia Router is restarted the WAN link and the routing table remain unaffected.

A single setting in the **Advanced Connection Options** screen controls this feature, as shown below.



When you toggle **Configuration Changes Reset WAN Connection** either to Yes or No using the Tab key and press Return, a pop-up window asks you to confirm your choice.

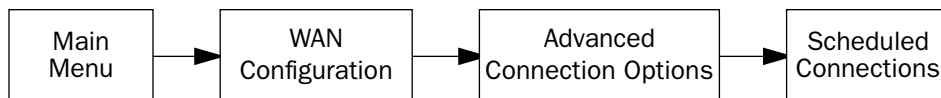


Toggling from **Yes** to **No** makes the router ready to be configured. If you toggle from **No** to **Yes** after any configuration changes have been entered (and confirm the reboot), your changes are committed and the router comes up using the newly created configuration.

Scheduled Connections

Scheduled connections are useful for PPPoE, PPTP, and ATMP connection profiles.

To go to the Scheduled Connections screen, from the WAN Configuration screen select **Advanced Connection Options** and then select **Scheduled Connections**.



Scheduled Connections

Display/Change Scheduled Connection...

Add Scheduled Connection...

Delete Scheduled Connection...

Navigate from here to add/modify/change/delete Scheduled Connections.

Viewing scheduled connections

To display a table of scheduled connections, select **Display/Change Scheduled Connection** in the Scheduled Connections screen. Each scheduled connection occupies one row of the table.

Scheduled Connections						
+Days-----	Begin At---	HH:MM---	When----	Conn. Prof. Name----	Enabled-----	+
mtWtfss	08:30PM	06:00	weekly	Profile 01	No	

The first column in the table shows a one-letter representation of the **Days** of the week, from Monday (M or m) to Sunday (S or s). If a letter representing a day is capitalized, the connection will be activated on that day; a lower-case letter means that the connection will not be activated on that day. If the scheduled connection is configured for a once-only connection, the word “once” will appear instead of the days of the week.

The other columns show:

- The time of day that the connection will **Begin At**
- The duration of the connection (**HH:MM**)
- Whether it's a recurring **Weekly** connection or used **Once Only**
- Which connection profile (**Conn. Prof.**) is used to connect
- Whether the scheduled connection is currently **Enabled**

The Router checks the date and time set in scheduled connections against the system date and time.

Adding a scheduled connection

To add a new scheduled connection, select **Add Scheduled Connection** in the Scheduled Connections screen and press Return. The Add Scheduled Connection screen appears.

Add Scheduled Connection

Scheduled Connection Enable:	On
How Often...	Weekly
Schedule Type...	Forced
Set Weekly Schedule...	
Use Connection Profile...	

ADD SCHEDULED CONNECTION
CANCEL

Scheduled Connections dial remote Networks on a Weekly or Once-Only basis.

Follow these steps to configure the new scheduled connection:

- To activate the connection, select **Scheduled Connection Enable** and toggle it to **On**. You can make the scheduled connection inactive by toggling **Scheduled Connection Enable** to **Off**.
- Decide how often the connection should take place by selecting **How Often** and choosing **Weekly** or **Once Only** from the pop-up menu.
- The **Schedule Type** allows you to set the exact weekly schedule or once-only schedule.

Options are:

- **Forced Up**, meaning that this connection will be maintained whether or not there is a demand call on the line.
- **Forced Down**, meaning that this connection will be torn down or blocked whether or not there is a demand call on the line.
- **Demand-Allowed**, meaning that this schedule will permit a demand call on the line.

- **Demand-Blocked**, meaning that this schedule will prevent a demand call on the line.
- **Periodic**, meaning that the connection is retried several times during the scheduled time.
- **Random Retry**, which operates as follows:

First, it will wait 0 to 60 seconds before starting, then it will try three times to bring the connection up as quickly as possible;

Second, on each successive retry after these first three attempts it will wait a random number of seconds between zero and a user-specified maximum.

Should the connection come up, and subsequently go down, the Scheduled Connection will start over with three retries. Switched connections have a variable redial back-off time depending on the interface type. Consequently, the first three attempts for such connections will be slower. Once the connection is up it will be forced to remain up.

- If **How Often** is set to **Weekly**, the item directly below **How Often** reads **Set Weekly Schedule**. If **How Often** is set to **Once Only**, the item directly below **How Often** reads **Set Once-Only Schedule**.

Set Weekly Schedule

If you set **How Often** to **Weekly**, select **Set Weekly Schedule** and go to the Set Weekly Schedule screen.

- Select the days for the scheduled connection to occur and toggle them to **Yes**.

Set Weekly Schedule

Monday:	No
Tuesday:	No
Wednesday:	No
Thursday:	No
Friday:	No
Saturday:	No
Sunday:	No
Scheduled Window Start Time:	04:29
AM or PM:	AM
Scheduled Window Duration Per Day:	00:00
Retry interval (minutes):	5

Return/Enter accepts * Tab toggles * ESC cancels.

- Select **Scheduled Window Start Time** and enter the time to initiate the scheduled connection.
- You must enter the time in the format H:M, where H is a one- or two-digit number representing the hour and M is a one- or two-digit number representing the minutes. The colon is mandatory. For example, the entry 1:3 (or 1:03) would be accepted as 3 minutes after one o'clock. The entry 7:0 (or 7:00) would be accepted as seven o'clock, exactly. The entries 44, :5, and 2: would be rejected.
- Select **AM or PM** and choose **AM** or **PM** from the pop-up menu.

- Select **Scheduled Window Duration Per Day** and enter the maximum duration allowed for this scheduled connection, per call.
- **Retry interval (minutes)** becomes visible if you have selected Random Retry. This option allows you to set the upper limit for the number of minutes to use for the retry time (the attempts after the first three attempts). It accepts values of 1 – 255 minutes; the default setting is 5 minutes. With a setting of 5 minutes it will try every 0 – 300 seconds after the first three retries to bring up the connection.

You are finished configuring the weekly options. Return to the Add Scheduled Connection screen to continue.

Set Once-Only Schedule

If you set **How Often** to **Once Only**, select **Set Once-Only Schedule** and go to the Set Once-Only Schedule screen.

Set Once-Only Schedule

Place Call on (MM/DD/YY):	05/07/1998
Scheduled Window Start Time: AM or PM:	11:50 AM
Scheduled Window Duration:	00:00

- Select **Place Call On (Date)** and enter a date in the format MM/DD/YY or MM/DD/YYYY (month, day, year).

Note: You must enter the date in the format specified. The slashes are mandatory. For example, the entry 5/7/98 would be accepted as May 7, 1998. The entry 5/7 would be rejected.

- Select **Scheduled Window Start Time** and enter the time to initiate the scheduled connection.

Note: You must enter the time in the format H:M, where H is a one- or two-digit number representing the hour and M is a one- or two-digit number representing the minutes. The colon is mandatory. For example, the entry 1:3 (or 1:03) would be accepted as 3 minutes after one o'clock. The entry 7:0 (or 7:00) would be accepted as seven o'clock, exactly. The entries 44, :5, and 2: would be rejected.

- Select **AM or PM** and choose **AM** or **PM**.
- Select **Scheduled Window Duration** and enter the maximum duration allowed for this scheduled connection. Use the same format restrictions noted above.

You are finished configuring the once-only options. Return to the Add Scheduled Connection screen to continue.

- In the Add Scheduled Connection screen, select **Use Connection Profile** and choose from the list of connection profiles you have already created. A scheduled connection must be associated with a connection profile to be useful. The connection profile becomes active during the times specified in the associated scheduled connection, if any exists.
- Select **ADD SCHEDULED CONNECTION** to save the current scheduled connection. Select **CANCEL** to exit the Add Scheduled Connection screen without saving the new scheduled connection.

Modifying a scheduled connection

To modify a scheduled connection, select **Display/Change Scheduled Connection** in the Scheduled Connections screen to display a table of scheduled connections.

Select a scheduled connection from the table and press Return. The Change Scheduled Connection screen appears. The parameters in this screen are the same as the ones in the Add Scheduled Connection screen (except that **ADD SCHEDULED CONNECTION** and **CANCEL** do not appear). To find out how to set them, see [“Adding a scheduled connection” on page 2-17](#).

Deleting a scheduled connection

To delete a scheduled connection, select **Delete Scheduled Connection** in the Scheduled Connections screen to display a table of scheduled connections.

Select a scheduled connection from the table and press the Return key to delete it. To exit the table without deleting the selected scheduled connection, press the Escape key.

Backup Configuration

See [“Line Backup” on page 7-1](#).

Priority Queuing (TOS bit)

Netopia Firmware Version 8.4 offers the ability to prioritize delay-sensitive data over the WAN link.

Certain types of IP packets, such as voice or multimedia packets, are sensitive to latency introduced by the network. This means that if such packets are not received rapidly, the quality of service degrades. If you expect to route significant amounts of such traffic you can configure your router to prioritize this type of traffic using the priority queuing feature.

To configure your router to prioritize delay-sensitive data, navigate to the Advanced Connection Options screen in the console menu.



The Advanced Connection Options screen appears.

Advanced Connection Options

Scheduled Connections...

Backup Configuration...

Prioritize Delay-Sensitive Data: No

Return/Enter to configure SA Backup Parameters.

The Router will recognize a delay-sensitive packet as having the low-latency bit set in the TOS field of the IP header.

If you toggle **Prioritize Delay-Sensitive Data** to **Yes** the router will place these packets at the front of the transmission queue to the WAN link, overtaking non-delay-sensitive traffic. Accepting the default **No** will allow the normal sequential queue of data packets.

System Configuration Screens

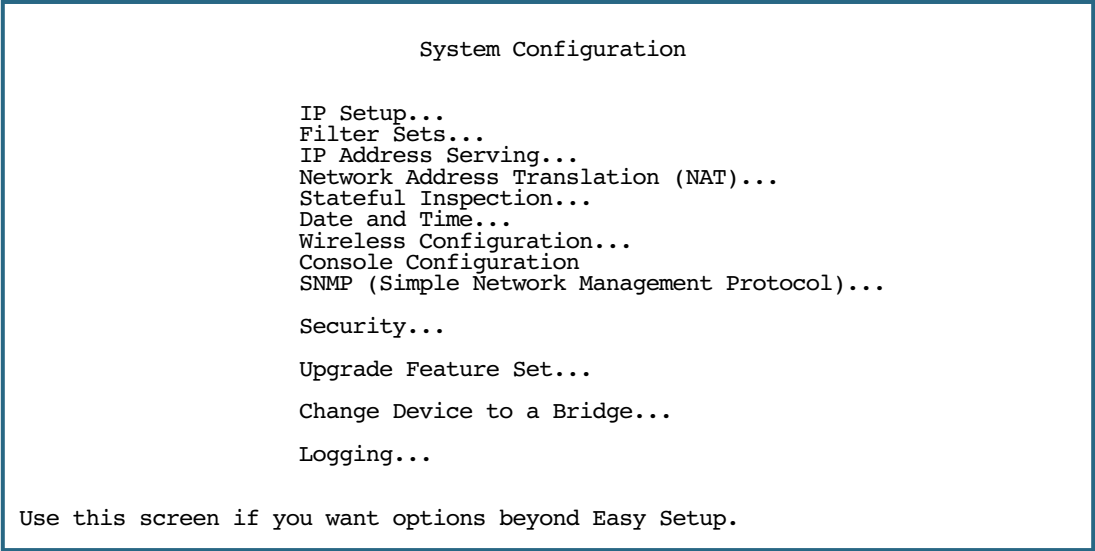
System configuration features

The Netopia Router’s default settings may be all you need to configure. Some users, however, require advanced settings or prefer manual control over the default selections. For these users, the Netopia Firmware Version 8.4 provides system configuration options.

“IP Setup” on page 2-23	“SNMP (Simple Network Management Protocol)” on page 2-36
“Filter Sets” on page 2-23	“Security” on page 2-36
“Network Address Translation (NAT)” on page 2-23	“Upgrade Feature Set” on page 2-36
“Stateful Inspection” on page 2-23	“Change Device to a Bridge” on page 2-37
“Date and time” on page 2-29	“Logging” on page 2-38
“Wireless configuration” on page 2-30	

To access the system configuration screens, select **System Configuration** in the Main Menu, then press Return.

The System Configuration menu screen appears:



IP Setup

These screens allow you to configure your network's use of the IP networking protocol.

- Details are given in [“IP Setup” on page 6-2](#).

Filter Sets

These screens allow you to configure security on your network by means of filter sets and a basic firewall.

- Details are given in [“Security” on page 9-1](#).

IP Address Serving

These screens allow you to configure IP address serving on your network by means of DHCP, WANIP, and BootP.

- Details are given in [“IP Address Serving” on page 6-17](#).

Network Address Translation (NAT)

These screens allow you to configure the Multiple Network Address Translation (MultiNAT) features.

- Details are given in [“Multiple Network Address Translation” on page 3-1](#).

Stateful Inspection

Stateful inspection is a security feature that prevents unsolicited inbound access when NAT is disabled. You can configure UDP and TCP “no-activity” periods that will also apply to NAT time-outs if stateful inspection is enabled on the interface. Stateful Inspection parameters are active on a WAN interface only if enabled on your Gateway. Stateful inspection can be enabled on a profile whether NAT is enabled or not.

Stateful Inspection

UDP no-activity timeout (sec): 180
TCP no-activity timeout (sec): 14400
Add Exposed Address List...

Exposed Address Associations...

Return/Enter goes to new screen.
Return/Enter to configure Xposed IP addresses.

- **UDP no-activity time-out:** The time in seconds after which a UDP session will be terminated, if there is no traffic on the session.
- **TCP no-activity time-out:** The time in seconds after which an TCP session will be terminated, if there is no traffic on the session.
- **Exposed Addresses:** The hosts specified in Exposed addresses will be allowed to receive inbound traffic even if there is no corresponding outbound traffic. This is active only if NAT is disabled on an WAN interface.

Stateful Inspection Options

Enable and configure stateful inspection on a WAN interface.

IP Profile Parameters

Address Translation Enabled:

Yes

IP Addressing...

Numbered

NAT Map List...

Easy-PAT List

NAT Server List...

Easy-Servers

NAT Options...

Stateful Inspection Enabled:

No

Local WAN IP Address:

0.0.0.0

Local WAN IP Mask:

0.0.0.0

Filter Set...

Remove Filter Set

RIP Profile Options...

Return/Enter to select <among/between> ...

Configure IP requirements for a remote network connection here.

When you create or modify a Connection Profile, the IP Profile Parameters screen allows you to enable Stateful Inspection on that profile by toggling **Stateful Inspection Enabled** to **Yes**. By default, this is turned off (No). If you enable Stateful Inspection, the Stateful Inspection Options field appears.

IP Profile Parameters	
Address Translation Enabled:	No
IP Addressing...	Numbered
Stateful Inspection Enabled:	Yes
Stateful Inspection Options...	
Local WAN IP Address:	0.0.0.0
Local WAN IP Mask:	0.0.0.0
Filter Set...	
Remove Filter Set	
RIP Profile Options...	
Configure IP requirements for a remote network connection here.	

Select **Stateful Inspection Options** and press Return. The Stateful Inspection Parameters screen appears.

Stateful Inspection Parameters	
Max. TCP Sequence Number Difference:	0
Enable default mapping to router:	No
Deny Fragmented Packets:	No
Exposed Address List...	
Enter max. allowed TCP sequence number difference (1 - 65535), 0 to disable.	

- **Max. TCP Sequence Number Difference:** Enter a value in this field. This value represents the maximum sequence number difference allowed between subsequent TCP packets. If this number is exceeded, the packet is dropped. The acceptable range is 0 – 65535. A value of 0 (zero) disables this check.
- **Enable default mapping to router:** This is disabled by default. Toggling this option to **Yes** will allow the router to respond to traffic received on this interface, for example, ICMP Echo requests.

Note: If Stateful Inspection is enabled on a base connection profile (for example, for PPP, RFC1483 bridged/routed, or PPPoE), **Enable default mapping to router** must be **yes** to allow inbound VPN terminations. (for example. for PPTP/ATMP client access to the router)

- **Deny Fragmented Packets:** Toggling this option to **Yes** causes the router to discard fragmented packets on this interface.
- You can apply these parameters to your Exposed Address lists by selecting your **Exposed Address List** from the pop-up menu,

Stateful Inspection Parameters

+Exposed Address List N+

Max. TCP Sequ	my_xposed_list	0
Enable default	<<None>>	No
Deny Fragment		No
Exposed Addre		

Up/Down Arrows to select, then Return/Enter; ESC to cancel.

Exposed Addresses

You can specify the IP addresses you want to expose by selecting **Add Exposed Address List** and pressing Return. The Add Exposed Address List screen appears.

Add Exposed Address List

Exposed Address List Name:my_xposed_addr_list

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.

Add, Edit, or delete exposed addresses options are active only if NAT is disabled on an WAN interface. The hosts specified in exposed addresses will be allowed to receive inbound traffic even if there is no corresponding outbound traffic.

Change Exposed Address Range ("my_xposed_list")

First Exposed Address:192.168.1.10

Last Exposed Address:-----+

Protocol...+-----+TCP and UDPTCPUDPANY

Port Start:

Port End:-----+

CHANGE EXPOSED ADDRESS RANGE

CANCEL

- **Start Address:** Start IP Address of the exposed host range.
- **End Address:** End IP Address of the exposed host range

2-28 *Firmware User Guide*

- **Protocol:** Select the Protocol of the traffic to be allowed to the host range from the pull-down menu. Options are Any, TCP, UDP, or TCP/UDP.
- **Start Port:** Start port of the range to be allowed to the host range. The acceptable range is from 1 - 65535
- **End Port:** Protocol of the traffic to be allowed to the host range. The acceptable range is from 1 - 65535

You can edit or delete exposed address lists by selecting **Show/Change Exposed Address List** or **Delete Exposed Address List**. A list of previously configured exposed addresses appears.

Add Exposed Address List

-----Exposed Address Range-----	-----Protocol-----
192.168.1.10 192.168.1.12	TCP and UDP

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

This allows you to select an exposed address list for editing or deletion.

Date and time

You can set the system's date and time parameters in the Set Date and Time screen.

Select **Date and Time** in the System Configuration screen and press Return. The Set Date and Time screen appears.

Set Date and Time

NTP (Network Time Prot.) Enabled:	On
Time Server Host Name/IP Address	204.152.184.72
Time Zone...	GMT -8:00 Pacific Standard Time
NTP Update Interval (HHHH:MM)	0:00
System Date Format:	MM/DD/YY
System Time Format:	AM/PM

Follow these steps to set the system's date and time:

1. Toggle **NTP (Network Time Prot.) Enabled** to On to synchronize the Router's time and date with a network server. Toggle this field to Off to manually set the time and date; the options in this screen will change to allow you to manually enter the time and date parameters.

Note: If time and date are manually set, that information will be lost upon reboot or loss of power.

2. Enter the IP address of the time server in the field **Time Server Host Name/IP Address**.
3. Select the Router's time zone from the **Time Zone** pop-up menu and press Return.
4. In the **NTP Update Interval** field, enter how often to synchronize with the time server, using the format HHHH:MM where H is hours and M is minutes.
5. Select a **System Date Format**; the options are MM/DD/YY, DD/MM/YY, and YY/MM/DD, where M is month, D is day, and Y is year.
6. Select a **System Time Format**, either AM/PM or 24hrs.
7. Press Escape to return to the System Configuration menu.

Note: NTP can be blocked by some firewall configurations. To ensure that this feature works, create a filterset rule to allow UDP port 123 to be open.

Wireless configuration

If your Router is a wireless model (such as a 3347W) you can enable or disable the wireless LAN by selecting **Wireless Configuration**. The Wireless Configuration screen appears.

Wireless LAN Configuration

Enable Wireless:	Yes
Enable Segmentation:	No
SSID:	5247 3521
Channel...	6
Closed System...	Open
Enable Privacy...	Off

Wireless MAC Authentication...

Return/Enter accepts * Tab toggles * ESC cancels.

Enable Wireless is set to **Yes** by default. When **Enable Wireless** is disabled (**No**), the Gateway will not provide or broadcast any wireless LAN services. If you toggle Enable Wireless to **No** or **Yes**, you must restart the Gateway for the change to take effect. See [“Restarting the System” on page 10-8](#).

Segmentation

- Enable Segmentation:** This feature isolates the hosts on the wireless LAN from the hosts on the wired Ethernet LAN. It also prevents the hosts on the wireless LAN from entering or enabling any VPN terminated on the Netopia Gateway.

If **on** is specified, the wireless LAN will be isolated from the wired LAN; if **off** is specified, the wireless LAN will be joined with the wired LAN.

You must reboot the unit for this setting to take effect.

- SSID** (Wireless ID): The SSID is preset to a number that is unique to your unit. You can either leave it as is, or change it by entering a freeform name of up to 32 characters, for example “Ed’s Wireless LAN”. On client PCs’ software, this might also be called the *Network Name*. The SSID is used to identify this particular wireless LAN. Depending on their operating system or client wireless card, users must either:
 - select from a list of available wireless LANs that appear in a scanned list on their client
 - or, if you are in Closed System Mode (see “Closed System” on [page 2-31](#)), enter this name on their clients in order to join this wireless LAN.

You can then configure:

- Channel:** (1 through 11) on which the network will broadcast. This is a frequency range within the 2.4Ghz band. Channel selection depends on government regulated radio frequencies that vary from region to

region. The widest range available is from 1 to 14. However, in North America only 1 to 11 may be selected. Europe, France, Spain and Japan will differ. Channel selection can have a significant impact on performance, depending on other wireless activity close to this Gateway. Channel selection is not necessary at the client computers; the clients will scan the available channels seeking access points using the same ESSID as the client.

- **Closed System:** If you toggle **Closed System** to **Closed**, the wireless network is hidden from the scanning features of wireless client computers. Unless both the wireless clients and the Router share the same SSID in Closed System mode, the Router's wireless LAN will not appear as an available network when scanned for by wireless-enabled computers. Members of the Closed System WLAN must log onto the Router's wireless network with the identical SSID as that configured in the router.

Closed System mode is an ideal way to increase wireless security and to prevent casual detection by unwanted neighbors, office users, or malicious users such as hackers.

If you toggle it to **Open**, it is more convenient, but potentially less secure, for clients to access your WLAN by scanning available access points. You must decide based on your own network requirements.

Note: Enabling Closed System Mode on your wireless Gateway provides another level of security, since your wireless LAN will no longer appear as an available access point to client PCs that are casually scanning for one.

Your own wireless network clients, however, must log into the wireless LAN by using the exact SSID of the Netopia Gateway.

In addition, if you have enabled WEP encryption on the Netopia Gateway, your network clients must also have WEP encryption enabled, and must have the same WEP encryption key as the Netopia Gateway.

Once the Netopia Gateway is located by a client computer, by setting the client to a matching SSID, the client can connect immediately if WEP is not enabled. If WEP is enabled then the client must also have WEP enabled and a matching WEP key.

Wireless client cards from different manufacturers and different operating systems accomplish connecting to a wireless LAN and enabling WEP in a variety of ways. Consult the documentation for your particular wireless card and/or operating system.

Enable Privacy

By default, **Enable Privacy** is set to **Off**. IT IS STRONGLY RECOMMENDED THAT YOU ENABLE PRIVACY.

- **WPA-PSK:** (Wi-Fi Protected Access) The easiest way to enable Privacy on your Wireless network is by selecting **WPA-PSK - (Pre-Shared Key)** from the pop-up menu.

Wireless LAN Configuration

Enable Wireless:

Yes

Enable Segmentation:

No

SSID:

5247 3521

Channel...

+-----+

Closed System...

+-----+

Enable Privacy...

Off

WEP - Manual

WEP - Automatic

WPA - PSK (Pre-Shared Key)

+-----+

Wireless MAC Authentication...

The **Pre Shared Key** field becomes visible to allow you to enter a Pre Shared Key. The key can be between 8 and 63 characters, but for best security it should be at least 20 characters. Clients wishing to connect must also be configured to use WPA with this same key.

Wireless LAN Configuration

Enable Wireless:

Yes

Enable Segmentation:

No

SSID:

5247 3521

Channel...

6

Closed System...

Open

Enable Privacy...

WPA - PSK (Pre-Shared Key)

Pre Shared Key:

Wireless MAC Authentication...

Select an 8 to 63 character passphrase. At least 20 is ideal for best security.

- WEP:** Alternatively, you can provide a level of data security by enabling WEP (Wired Equivalent Privacy) for encryption of network data. You can enable 40-, 128-, or 256-bit WEP Encryption (depending on the capability of your client wireless card) for IP traffic on your LAN.

Wireless LAN Configuration

```

Enable Wireless:                Yes

SSID:                          4405 2605
Channel...                     6
Closed System...               Open
Enable WEP...                  On - Automatic

Default Key...                 1
Passphrase:    Well I stand up next to a mountain,

Key 1 (40b): 5ad06701b4
Key 2 (128b): 80a6ab74749ea5a251011d8979
Key 3 (128b): e024cb9417a521b0e49e208fef
Key 4 (40b): 46a968d564

```

Enter a phrase and hit Enter to generate your encryption keys.

You select a single key for encryption of outbound traffic. The WEP-enabled client must have an identical key of the same length, in the identical slot (1 – 4) as the Gateway, in order to successfully receive and decrypt the traffic. Similarly, the client also has a ‘default’ key that it uses to encrypt its transmissions. In order for the Gateway to receive the client’s data, it must likewise have the identical key of the same length, in the same slot. For simplicity, a Gateway and its clients need only enter, share, and use the first key.

The pull-down menu for enabling WEP offers these settings: **On - Automatic** or **On - Manual**.

- **On - Automatic** uses a passphrase to generate encryption keys for you. You enter a passphrase that you choose in the Passphrase field. The passphrase can be any string of words or numbers.

Note: While clients may also have a passphrase feature, these are vendor-specific and may not necessarily create the same keys. You can passphrase generate a set of keys on one, and manually enter them on the other to get around this.

Select the **Default Key** (#1 – #4). The longer the key, the stronger the encryption and the more difficult it is to break the encryption.

- **On - Manual** allows you to enter your own encryption keys manually. This is a difficult process, but only

needs to be done once. Avoid the temptation to enter all the same characters.

Wireless LAN Configuration

Enable Wireless:

Yes

SSID:

4405 2605

Channel...

6

Closed System...

Open

Enable WEP...

On - Manual

Default Key...

1

+-----+

+-----+

Key

40 bit

9a82ff3d92

Key

128 bit

2f5d42db7b734ff4e17b65881e

Key

256 bit

db298860b6f380e6daec7dbfd4

Key

+-----+

c8e5281016

(Setting one of the key sizes)

Default Key (#1 – #4): Specifies which key the Router will use to encrypt transmitted traffic. The default is key #1.

Key (#1 – #4): The encryption keys. You enter keys using hexadecimal digits. For 40/64bit encryption, you need ten digits; 26 digits for 128bit, and 58 digits for 256bit WEP. Hexadecimal characters are 0 – 9, and a – f. The longer the key, the stronger the encryption and the more difficult it is to break the encryption.

Examples:

- 40bit: 02468ACE02
- 128bit: 0123456789ABCDEF0123456789
- 256bit: 592CA140F0A238B0C61AE162F592CA140F0A238B0C61AE162F21A09C

Wireless MAC Authentication

Wireless MAC Authentication allows you to specify which client PCs are allowed to join the wireless LAN by specific hardware address. Once it is enabled, only entered MAC addresses that have been set to Allow will be accepted onto the wireless LAN. All unlisted addresses will be blocked, in addition to the listed addresses with Allow disabled.

To enable Wireless MAC Authentication, select Wireless MAC Authentication, and press Return.

The Wireless MAC Authorization screen appears.

Authorized Wireless MAC Addresses

Enable MAC Authentication: Yes

Display/Change MAC Addresses...

Add MAC Address...

Delete MAC Address...

To enable Wireless Mac Authorization, toggle **Enable MAC Authentication** to **Yes**. You can toggle it to **No** to disable it at any time.

Select **Add MAC Address** and press Return. The Add Wireless MAC Address screen appears.

Add Wireless MAC Address

Wireless MAC Allowed: Yes

Wireless MAC Address: 00-0a-27-ae-71-a4

ADD WIRELESS MAC NOW CANCEL

Return/Enter accepts * Tab toggles * ESC cancels.
Configure a new Wireless MAC in this Screen.

Enter the MAC (hardware) address of the client PC you want to authorize for access to your wireless LAN. **Wireless MAC Allowed** is set to **Yes** (enabled) by default. Toggling this to **No** (disabled) specifically denies access from this MAC address.

Select **ADD WIRELESS MAC NOW**, and press Return.

2-36 *Firmware User Guide*

Your entry will be added to a list of up to 32 authorized addresses. To display the list of authorized MAC addresses, select **Display/Change MAC Addresses** from the Authorized Wireless MAC Addresses menu.

The list is displayed as shown below.

+--MAC Address -----	Permission -----
00-0a-27-ae-71-a4	Allowed
00-0b-28-af-72-b5	Allowed
00-0c-29-bd-69-b3	Blocked

Select an address to modify.

You can continue to **Add**, **Change**, or **Delete** addresses to the list by selecting the respective menu options.

SNMP (Simple Network Management Protocol)

These screens allow you to monitor and configure your network by means of a standard Simple Network Management Protocol (SNMP) agent.

- Details are given in [“Simple Network Management Protocol \(SNMP\)” on page 8-10](#).

Security

These screens allow you to add users and define passwords on your network.

- Details are given in [“Security” on page 9-1](#).

Upgrade Feature Set

You can upgrade your Netopia Router by adding new feature sets through the Upgrade Feature Set utility.

See the release notes that came with your Router or feature set upgrade, or visit the Netopia Web site at www.netopia.com for information on new feature sets, how to obtain them, and how to install them on your Router.

Change Device to a Bridge

For Netopia DSL Routers, this feature allows you to turn off the routing features and use your device as a bridge. It is not an option for Ethernet WAN models. If you select this option, the device will restart itself, and reset all the settings to factory defaults. Any configurations you have made will be erased. Use this feature with caution. If you decide to reinstate the routing capabilities, you must reconfigure the device from scratch.

From the **Main Menu**, select **System Configuration**.

```

                                System Configuration

IP Setup...
Filter Sets...
IP Address Serving...
Network Address Translation (NAT)...

Date and Time...

SNMP (Simple Network Management Protocol)...

Security...

Upgrade Feature Set...

Change Device to a Bridge...

Logging...

Use this screen if you want options beyond Easy Setup.

```

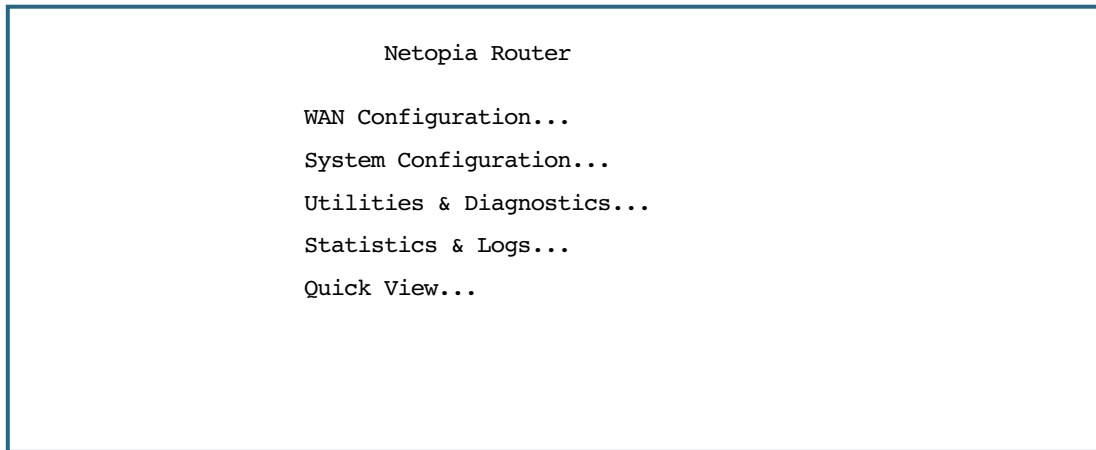
Select **Change Device to a Bridge** and press **Return**. You will be challenged to confirm this choice.

```

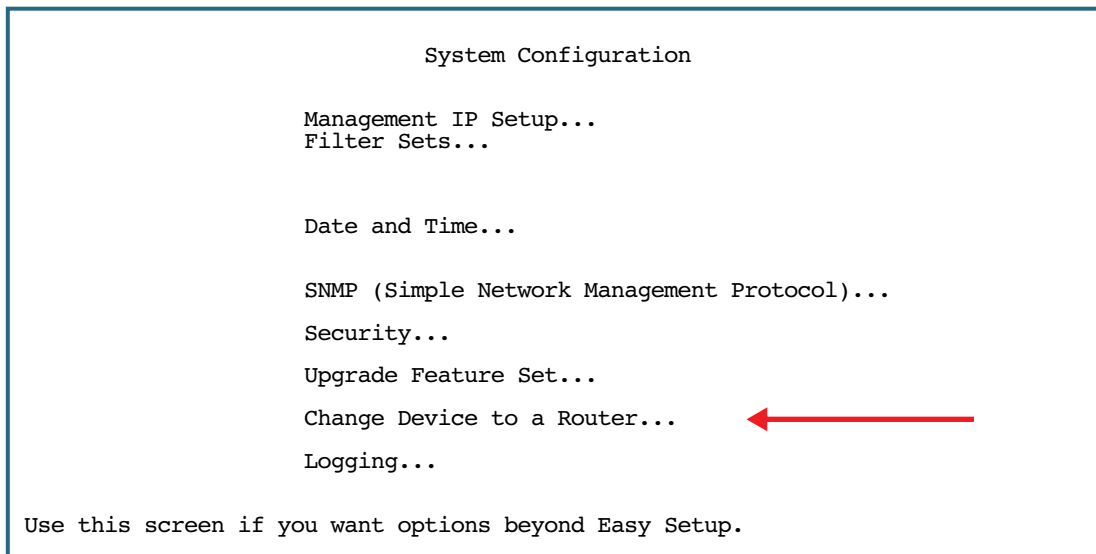
+-----+
+-----+
| This change requires a reboot and will result |
| in Factory Defaulting the device.             |
|                                         CANCEL          CONTINUE |
+-----+
+-----+

```

If you chose **CONTINUE**, the device will reboot and restart in bridge mode. Routing features will be disabled and the Telnet menus corresponding configuration items, such as Easy Setup, will be removed.



You can reinstate Router mode by returning to the System Configuration menu.



Select **Change Device to a Router**.

Press **Return**, confirm your choice, and the device will restart in router mode.

Logging

You can configure a UNIX-compatible syslog client to report a number of subsets of the events entered in the Router's WAN Event History. See [“WAN Event History” on page 8-5](#).

The Syslog client (for the PC only) is available on the Netopia CD.

Select **Logging** from the System Configuration menu.

The Logging Configuration screen appears.

Logging Configuration	
WAN Event Log Options	
Log Boot and Errors:	Yes
Log Line Specific:	Yes
Log Connections:	Yes
Log PPP, DHCP, CNA:	Yes
Log IP:	Yes
Syslog Parameters	
Syslog Enabled:	No
Hostname or IP Address:	
Facility...	Local 0

By default, all events are logged in the event history.

- By toggling each event descriptor to either **Yes** or **No**, you can determine which ones are logged and which are ignored.
- You can enable or disable the syslog client dynamically. When enabled, it will report any appropriate and previously unreported events.
- You can specify the syslog server's address either in dotted decimal format or as a DNS name up to 63 characters.
- You can specify the UNIX syslog Facility to use by selecting the **Facility** pop-up.
- Erase the log by selecting DUMP WAN LOG

You will need to install a Syslog client daemon program on your PC and configure it to report the WAN events you specified in the Logging Configuration screen.

The following screen shows a sample syslog dump of WAN events:

```

May  5 10:14:06 tsnext.netopia.com    Link 1 down: PPP PAP failure
May  5 10:14:06 tsnext.netopia.com    >>Issued Speech Setup Request from our DN: 5108645534
May  5 10:14:06 tsnext.netopia.com    Requested Disc. from DN: 917143652500
May  5 10:14:06 tsnext.netopia.com    Received Clear Confirm for our DN: 5108645534
May  5 10:14:06 tsnext.netopia.com    Link 1 down: Manual disconnect
May  5 10:14:06 tsnext.netopia.com    >>Issued Speech Setup Request from our DN: 5108645534
May  5 10:14:06 tsnext.netopia.com    Requested Disc. from DN: 917143652500
May  5 10:14:06 tsnext.netopia.com    Received Clear Confirm for our DN: 5108645534
May  5 10:14:06 tsnext.netopia.com    Link 1 down: No answer
May  5 10:14:06 tsnext.netopia.com    --Device restarted-----
May  5 10:14:06 tsnext.netopia.com    >>Received Speech Setup Ind. from DN: (not supplied)
May  5 10:14:06 tsnext.netopia.com    Requested Connect to our DN: 5108645534
May  5 10:14:06 tsnext.netopia.com    ASYNC: Modem carrier detected (more) Modem
May  5 10:14:06 tsnext.netopia.com    reports: 26400 V34
May  5 10:14:06 tsnext.netopia.com    >>WAN: 56K Modem 1 activated at 115 Kbps
May  5 10:14:06 tsnext.netopia.com    Connect Confirmed to our DN: 5108645534
May  5 10:14:06 tsnext.netopia.com    PPP: Channel 1 up, Answer Profile name: Default Profile
May  5 10:14:06 tsnext.netopia.com    PPP: NCP up, session 1, Channel 1 Final (fallback)
May  5 10:14:06 tsnext.netopia.com    negotiated auth: Local PAP , Remote NONE
May  5 10:14:06 tsnext.netopia.com    PPP: PAP we accepted remote, Channel 1 Remote name: guest
May  5 10:14:06 tsnext.netopia.com    PPP: MP negotiated, session 1 Remote EDO: 06 03 0
May  5 10:14:06 tsnext.netopia.com    000C5700624 0
May  5 10:14:06 tsnext.netopia.com    PPP: CCP negotiated, session 1, type: Ascend
May  5 10:14:06 tsnext.netopia.com    LZS Local mode: 1, Remote mode: 1
May  5 10:14:06 tsnext.netopia.com    PPP: BACP negotiated, session 1 Local MN: FFFFFFFF
May  5 10:14:06 tsnext.netopia.com    FF, Remote MN: 00000001
May  5 10:14:06 tsnext.netopia.com    PPP: IPCP negotiated, session 1, rem:
May  5 10:14:06 tsnext.netopia.com    192.168.10.100 local: 192.168.1.1
May  5 10:14:06 tsnext.netopia.com    >>WAN: 56K Modem 1 deactivated
May  5 10:14:06 tsnext.netopia.com    Received Clear Ind. from DN: 5108645534, Cause: 0
May  5 10:14:06 tsnext.netopia.com    Issued Clear Response to DN: 5108645534
May  5 10:14:06 tsnext.netopia.com    Link 1 down: Remote clearing
May  5 10:14:06 tsnext.netopia.com    PPP: IPCP down, session 1
May  5 10:14:06 tsnext.netopia.com    >>Received Speech Setup Ind. from DN: (not supplied)

```


Chapter 3

Multiple Network Address Translation

Netopia Firmware Version 8.4 offers advanced Multiple Network Address Translation functionality.

You should read this chapter completely before attempting to configure any of the advanced NAT features.

This chapter covers the following topics:

- [Overview on page 3-1](#)
- [MultiNAT Configuration on page 3-6](#)
- [Easy Setup Profile configuration on page 3-6](#)
- [Server Lists and Dynamic NAT configuration on page 3-7](#)
- [Adding Server Lists on page 3-15](#)
- [Binding Map Lists and Server Lists on page 3-21](#)
- [NAT Associations on page 3-25](#)
- [IP Passthrough on page 3-27](#)
- [MultiNAT Configuration Example on page 3-31](#)

Overview

NAT (Network Address Translation) is a means of mapping one or more IP addresses and/or IP service ports into different values. This *mapping* serves two functions:

- It allows the addresses of many computers on a LAN to be represented to the public Internet by only one or a few addresses, saving you money.
- It can be used as a security feature by obscuring the true addresses of important machines from potential hackers on the Internet.

To help you understand some of the concepts discussed here, it may be helpful to introduce some NAT terminology.

The term *mapping* refers to rules that associate one or more private addresses on the Netopia Router's LAN to one or more public addresses on the Netopia Router's WAN interface (typically the Internet).

The terms *private* and *internal* refer to addresses on the Netopia Router's LAN. These addresses are considered private because they are protected or obscured by NAT and cannot be directly accessed from the WAN (or Internet) side of the Netopia Router unless specifically configured otherwise.

The terms *public* and *external* refer to the WAN (or Internet) side of the Netopia Router.

Features

MultiNAT features can be divided into several categories that can be used simultaneously in different combinations on a per-Connection Profile basis.

The following is a general description of these features:

Port Address Translation

The simplest form of classic Network Address Translation is *PAT* (Port Address Translation). PAT allows a group of computers on a LAN, such as might be found in a home or small office, to share a single Internet connection using one IP address. The computers on the LAN can surf the Web, read e-mail, download files, etc., but their individual IP addresses are never exposed to the public network. Instead, a single IP address acts as the source IP address of traffic originating from the LAN. The Netopia Router allows you to define multiple PAT mappings, which can be individually mapped to different public IP addresses. This offers more control over the access permitted to users on the LAN.

A limitation of PAT is that communication must be initiated from the internal network. A user on the external side cannot access a machine behind a PAT connection. A PAT enhancement is the ability to define multiple PAT mappings. Each of these can optionally map to a section or *range* of IP addresses of the internal network. PAT mapping allows only internal users to initiate traffic flow between the internal and external networks.

Server lists

Server lists, sometimes known as exported services, make it possible to provide access from the public network to hosts on the LAN. Server lists allow you to define particular services, such as Web, ftp, or e-mail, which are available via a public IP address. You define the type of service you would like to make available and the internal IP address to which you would like to provide access. You may also define a specific public IP address to use for this service if you want to use an IP other than the WAN IP address of the Netopia Router.

Static mapping

If you want to host your own Website or provide other Internet services to the public, you need more than classic NAT. The reason is noted under Port Address Translation above – external users cannot initiate traffic to computers on your LAN because external users can never see the real addresses of the computers on your LAN. If you want users outside your LAN to have access, for example, to a Web or FTP server that you host, you need to make a public representation of the real IP addresses of those servers.

Static mappings are a way to make one or more private IP addresses fully accessible from the public network via corresponding public IP addresses. Some applications may negotiate multiple TCP connections in the process of communication, which often does not work with traditional PAT. Static mapping offers the ability to use these applications through NAT. Each private IP address is mapped, on a one-to-one basis, to a public IP address that can be accessed from the Internet or public network. As with PAT mappings, you may have multiple static mappings to map a range of private IP addresses to a range of public IP addresses if desired.

Dynamic mapping

Dynamic mapping, often referred to as many-to-few, offers an extension to the advantages provided by static mapping. Instead of requiring a one-to-one association of public addresses and private addresses, as is required in static mapping, dynamic mapping uses a group of public IP addresses to dynamically allocate static mappings to private hosts that are communicating with the public network. If a host on the private network initiates a connection to the Internet, for example, the Netopia Router automatically sets up a one-to-one mapping of that host's private IP address to one of the public IP addresses allocated to be used for Dynamic NAT. As long as this host is communicating with the Internet, it will be able to use that address. When traffic from that host ceases, and no traffic is passed from that host for five minutes, the public address is made available again for other private hosts to use as necessary.

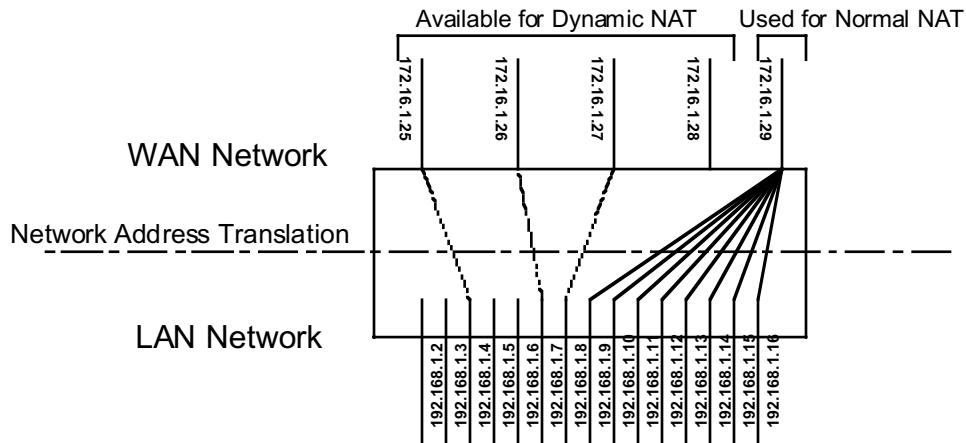
When addresses are returned to the group of available addresses, they are returned to the head of the group, being the most recently used. If that same host requests a connection an hour later, and the same public address is still available, then it will be mapped to the same private host. If a new host, which has not previously requested a connection, initiates a connection it is allocated the last, or oldest, public address available.

Dynamic NAT is a way of sharing a range of public, or exterior, NAT addresses among one or more *groups* of private, or interior, hosts. This is intended to provide superior support for applications that traditionally have difficulty communicating through NAT. Dynamic NAT is intended to provide functionality beyond many-to-one and one-to-one translation. Netopia's NAT implementation makes it possible to have a static mapping of one public address to one private address, thus allowing applications such as NetMeeting to work by assuring that any traffic sent back to the source IP address is forwarded through to the internal machine.

Static one-to-one mapping works well if you have enough IP addresses for all the workstations on your LAN. If you do not, Dynamic NAT allows machines to make full use of the publicly routable IP addresses provided by the ISP as necessary, on demand. When these public IP addresses are no longer being used by a particular workstation, they are returned to a pool of available addresses for other workstations to use.

A common example is a DSL customer's application. Most DSL ISPs only provide customers with a few IP addresses for use on their network. For networks with more than four or five machines it is usually mandatory to use NAT. A customer may have 15 workstations on the LAN, all of which need Internet access. The customer is only provided five IP addresses by their ISP. The customer has eight hosts, which only need to use email and have Web access, but another seven hosts, which use NetMeeting to communicate with clients once or twice a day. NetMeeting will not work unless a static one-to-one mapping exists for the machine running NetMeeting to use for communication. The customer does not have enough IP addresses to create a one-to-one mapping for each of the seven users. This is where dynamic NAT applies.

The customer can configure four of these addresses to be used for Dynamic NAT. The fifth address is then used for the eight other machines that do not need one-to-one mappings. As each machine configured to use addresses from the dynamic pool tries to connect to the Internet it is allocated a public IP address to use temporarily. Once the communication has been terminated, that IP address is freed for one of the other six hosts to use.



Exterior addresses are allocated to internal hosts on a demand, or as-needed, basis and then made available when traffic from that host ceases. Once an internal host has been allocated an address, it will use that address for all traffic. Five minutes after all traffic ceases – no pings, all TCP connections closed, no DNS requests, etc. – the address is put at the head of an *available* list. If an interior host needs an exterior address an hour later, and the previously used address is still available, it will acquire the same address. If an interior host that has not previously been allocated an exterior address needs one, it will be allocated the last, hence the oldest, exterior address on the available list.

All NAT configurations are *rule-based*. This means that traffic passed through NAT from either the public or the private network is compared to the rules and mappings configured in the Netopia Router in a particular order. The first rule that applies to the traffic being initiated is used.

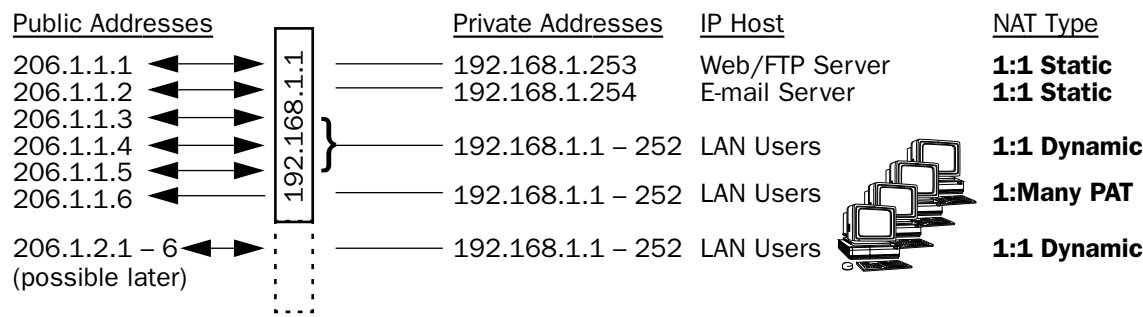
For example, if a connection is initiated from the public network and is destined for a public IP address configured on the Netopia Router, the following comparisons are made in this order.

1. The Netopia Router first checks its internal NAT cache to see if the data is part of a previously initiated connection, if not...
2. The Netopia Router checks the configured server lists to see if this traffic is intended to be forwarded to an internal host based on the type of service.
3. The Netopia Router then checks to see if there is a static, dynamic, or PAT mapping for the public IP address that the connection is being initiated to.
4. The Netopia Router answers the request itself if the data is destined for the Netopia's WAN interface IP address. Otherwise the data is discarded.

Complex maps

Map lists and server lists are completely independent of each other. A Connection Profile can use one or the other or both.

MultiNAT allows complex mapping and requires more complex configuration than in earlier firmware versions. Multiple mapped interior subnets are supported, and the rules for mapping each of the subnets may be different. The figure below illustrates a possible multiNAT configuration.



In order to support this type of mapping, you define two address ranges. First, you define a public range which contains the first and last public address to be used and the way in which these addresses should be used (PAT, static, or dynamic). You then configure an address map which defines the private IP address or addresses to be used and which public range they should be mapped to. You add the address map to the list of address maps which are configured, creating a map list. The mappings in the map list are order-dependent and are compared in order from the top of the list to the bottom. If a particular resource is not available, subordinate mappings can be defined that will redirect traffic.

Supported traffic

MultiNat supports the following IP protocols:

- PAT: TCP/UDP traffic which does not carry source or destination IP addresses or ports in the data stream (i.e., HTTP, Telnet, 'r' commands, tftp, NFS, NTP, SMTP, NNTP, etc.).
- Static NAT: All IP protocol traffic which does not carry or otherwise rely on the source or destination IP addresses in the data stream.
- Dynamic NAT: All IP protocol traffic which does not carry or otherwise rely on the source or destination IP addresses in the data stream.

Support for AOL Instant Messenger (AIM) File Transfer

Netopia Firmware Version 8.4 provides Application Level Gateway (ALG) support for AOL Instant Messenger (AIM) file transfer. This allows AIM users to exchange files, even when both users are behind NAT. Previously, the file transfer function would work only if one or neither of the two users were behind NAT.

Currently there is a restriction that the remote user must be routed to via the WAN interface, otherwise the connections will fail. There is no restriction as to the number of connections.

There is no user configuration required for this feature.

Support for Yahoo Messenger

Netopia Firmware Version 8.4 provides Application Level Gateway (ALG) support for Yahoo Messenger. This allows Yahoo Messenger users to exchange files, even when both users are behind NAT. Previously, the file transfer function would work only if one or neither of the two users were behind NAT.

Currently there is a restriction that the remote user must be routed to via the WAN interface, otherwise the connections will fail. There is no restriction as to the number of connections.

There is no user configuration required for this feature.

MultiNAT Configuration

You configure the MultiNAT features through the Telnet menu:

- For a simple 1-to-many NAT configuration (classic NAT or PAT), use the [Easy Setup Profile configuration](#), described below.
- For the more advanced features, such as server lists and dynamic NAT, follow the instructions in:
 - [IP setup](#), described on [page 3-7](#)
 - [IP profile parameters](#), described on [page 3-21](#)

Easy Setup Profile configuration

The screen below is an example. Depending on the type of Router you are using, fields displayed in this screen may vary.

Connection Profile 1: Easy Setup Profile

Connection Profile Name:

Easy Setup Profile

Address Translation Enabled:

Yes

IP Addressing...

Numbered

Local WAN IP Address:

0.0.0.0

Local WAN IP Mask:

255.255.255.0

Remote IP Address:

127.0.0.2

Remote IP Mask:

255.255.255.255

PPP Authentication...

PAP

Send User Name:

tonyf

Send Password:

PREVIOUS SCREEN

NEXT SCREEN

Return/Enter brings you to next screen.

The **Local WAN IP Address** is used to configure a NAT public address range consisting of the Local WAN IP Address and all its ports. The public address map list is named *Easy-PAT List* and the port map list is named *Easy-Servers*.

The two map lists, Easy-PAT List and Easy-Servers, are created by default and NAT configuration becomes effective. This will map all your private addresses (0.0.0.0 through 255.255.255.255) to your public address. These map lists are bound to the Easy Setup Profile. See [Binding Map Lists and Server Lists on page 3-21](#).

This is all you need to do if you want to continue to use a single PAT, or 1-to-many, NAT configuration.

Server Lists and Dynamic NAT configuration

You use the advanced NAT feature sets by first defining a series of mapping rules and then grouping them into a *list*. There are two kinds of lists – *map lists*, made up of dynamic, PAT and static mapping rules, and *server lists*, a list of internal services to be presented to the external world. Creating these lists is a four-step process:

1. **Define the public range** of addresses that external computers should use to get to the NAT internal machines. These are the addresses that someone on the Internet would see.
2. **Create a List name** that will act as a rule or server holder.
3. **Create a map or rule** that specifies the internal range of NATed addresses and the external range they are to be associated with.
4. **Associate the Map or Server List to your WAN interface** via a Connection Profile or the Default Profile.

The three NAT features all operate completely independently of each other, although they can be used simultaneously on the same Connection Profile.

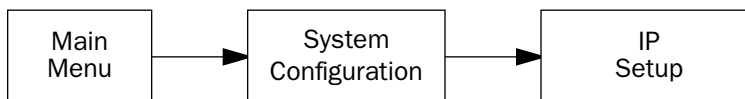
You can configure a simple 1-to-many PAT (often referred to simply as NAT) mapping using Easy Setup. More complex setups require configuration using the **Network Address Translation** item on the IP Setup screen.

An example MultiNAT configuration at the end of this chapter describes some applications for these features. See the [MultiNAT Configuration Example on page 3-31](#).

In order to configure the Router to make servers on your LAN visible to the Internet, you use advanced features in the System Configuration screens, described in [IP setup](#).

IP setup

To access the NAT configuration screens, from the Main Menu navigate to IP Setup:



IP Setup

Ethernet IP Address:	192.168.1.1
Ethernet Subnet Mask:	255.255.255.0
Define Additional Subnets...	
Default IP Gateway:	127.0.0.2
Primary Domain Name Server:	0.0.0.0
Secondary Domain Name Server:	0.0.0.0
Domain Name:	isp.com
Receive RIP...	Both
Transmit RIP...	Off

Static Routes... IP Address Serving...

Network Address Translation (NAT)...

Set up the basic IP attributes of your Netopia in this screen.

Select **Network Address Translation (NAT)** and press Return.

The Network Address Translation screen appears.

Network Address Translation

Add Public Range...
Show/Change Public Range...
Delete Public Range...

Add Map List...
Show/Change Map List...
Delete Map List...

Add Server List...
Show/Change Server List...
Delete Server List...

NAT Associations...

Return/Enter to configure IP Address redirection.

Public Range defines an external address range and indicates what type of mapping to apply when using this range. The types of mapping available are *dynamic*, *static* and *pat*.

Map Lists define collections of mapping rules. A rule maps interior range addresses to exterior range addresses by the mapping techniques defined in the map list.

Server Lists bind internal IP addresses and ports to external IP addresses and ports so that connections initiated from the outside can access an interior server.

NAT rules

The following rules apply to assigning NAT ranges and server lists:

- Static public address ranges must not overlap other static, PAT, public addresses, or the public address assigned to the Router's WAN interface.
- A PAT public address must not overlap any static address ranges. It may be the same as another PAT address or server list address, but the port range must not overlap.

You configure the ranges of exterior addresses by first adding public ranges.

Select **Add Public Range** and press Return.

The Add NAT Public Range screen appears.

Add NAT Public Range

Range Name:	my_first_range
Type...	pat
Public Address:	206.1.1.6
First Public Port:	49152
Last Public Port:	65535
<div style="display: flex; justify-content: space-around;"> ADD NAT PUBLIC RANGE CANCEL </div>	

- Select **Range Name** and give a descriptive name to this range.
- Select **Type** and from the pop-up menu, assign its type. Options are **static**, **dynamic**, or **pat** (the default).
 - If you choose **pat** as the range type, select **Public Address** and enter the exterior IP address in the range you want to assign. Select **First** and **Last Public Port** and enter the first and last exterior ports in the range. These are the ports that will be used for traffic initiated from the private LAN to the outside world.

Note: For PAT map lists and server lists, if you use the Public Address 0.0.0.0, the list will acquire its public IP address from the WAN IP address specified by your WAN IP configuration in the Connection Profile. If that is a static IP address, then the PAT map list and server lists will acquire that address. If it is a negotiated IP address, such as may be assigned via DHCP or PPP, the PAT map list and server lists will acquire that address each time it is negotiated.

- If you choose **dynamic** as the range type, a new menu item, **First Public Address**, becomes visible. Select **First Public Address** and enter the first exterior IP address in the range you want to assign. Select **Last Public Address** and enter an IP address at the end of the range.
- If you choose **static** as the range type, a new menu item, **First Public Address**, becomes visible.

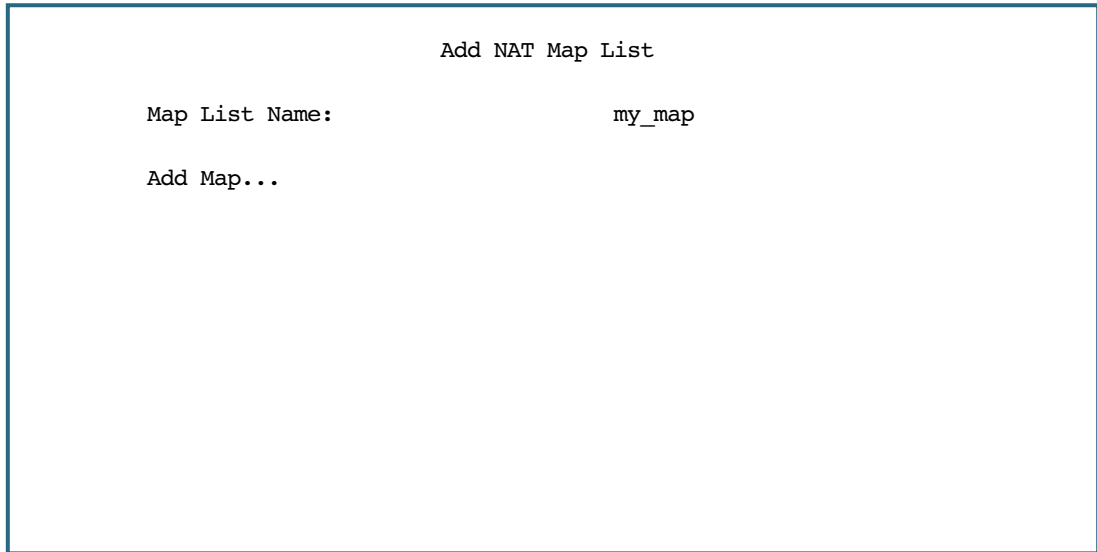
Select **First Public Address** and enter the first exterior IP address in the range you want to assign.
Select **Last Public Address** and enter an IP address at the end of the range.

- Select **ADD NAT PUBLIC RANGE** and press Return. The range will be added to your list and you will be returned to the Network Address Translation screen.

Once the public ranges have been assigned, the next step is to bind interior addresses to them. Because these bindings occur in ordered lists, called *map lists*, you must first define the list, then add mappings to it.

From the Network Address Translation screen select **Add Map List** and press Return.

The Add NAT Map List screen appears.



Add NAT Map List

Map List Name: my_map

Add Map...

- Select **Map List Name** and enter a descriptive name for this map list. A new menu item, **Add Map**, appears.
- Select **Add Map** and press Return. The Add NAT Map screen appears.

```

Add NAT Map ("my_map")

First Private Address:      192.168.1.1
Last Private Address:      192.168.1.254

Use NAT Public Range...

ADD NAT MAP                CANCEL

```

- Select **First** and **Last Private Address** and enter the first and last interior IP addresses you want to assign to this mapping.
- Select **Use NAT Public Range** and press Return. A screen appears displaying the public ranges you have defined.

```

Add NAT Map ("my_map")
+--Public Address Range-----Type-----Name-----+
+-----+-----+-----+-----+
0.0.0.0      --      pat      Easy-PAT
206.1.1.6    --      pat      my_first_range
206.1.1.1    206.1.1.2 static  my_second_range
<<NEW RANGE...>>
+-----+-----+-----+-----+

Up/Down Arrow Keys to select, ESC to cancel, Return/Enter to Delete.

```

Select ←

- From the list of public ranges you defined, select the one that you want to map to the interior range for this mapping and press Return.

If none of your preconfigured ranges are suitable for this mapping, you can select **<<NEW RANGE>>** and create a new range. If you choose **<<NEW RANGE>>**, the Add NAT Public Range screen displays and you can create a new public range to be used by this map. See [Add NAT Public Range on page 3-9](#).

- The Add NAT Map screen now displays the range you have assigned.

Add NAT Map ("my_map")

First Private Address:192.168.1.1

Last Private Address:192.168.1.254

Use NAT Public Range...my_first_range

Public Range Type is:pat

Public Range Start Address is:206.1.1.6

ADD NAT MAP

CANCEL

- Select **ADD NAT MAP** and press Return. Your mapping is added to your map list.

Modifying map lists

You can make changes to an existing map list after you have created it. Since there may be more than one map list you must select which one you are modifying.

From the Network Address Translation screen select **Show/Change Map List** and press Return.

- Select the map list you want to modify from the pop-up menu.

Network Address Translation

+--NAT Map List Name--+

Add Out

Show/Ch

Delete

Easy-PAT List

my_map

Add Map

Show/Ch

Delete

Add Ser

Show/Ch

Delete

NAT Ass

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

The Show/Change NAT Map List screen appears.

Show/Change NAT Map List

Map List Name:

my_map

Add Map...

Show/Change Maps...

Delete Map...

- **Add Map** allows you to add a new map to the map list.
- **Show/Change Maps** allows you to modify the individual maps within the list.
- **Delete Map** allows you to delete a map from the list.

Selecting **Show/Change Maps** or **Delete Map** displays the same pop-up menu.

Show/Change NAT Map List

Private Address Range		Type	Public Address Range	
192.168.1.1	192.168.1.254	pat	206.1.1.6	--
192.168.1.253	192.168.1.254	static	206.1.1.1	206.1.1.2
192.168.1.1	192.168.1.252	dynamic	206.1.1.3	206.1.1.5

Scroll to the map you want to modify using the arrow keys and press Return.

The Change NAT Map screen appears.

Change NAT Map ("my_map")

First Private Address:

192.168.1.253

Last Private Address:

192.168.1.254

Use NAT Public Range...

my_second_range

Public Range Type is:

static

Public Range Start Address is:

206.1.1.1

Public Range End Address is:

206.1.1.2

CHANGE NAT MAP

CANCEL

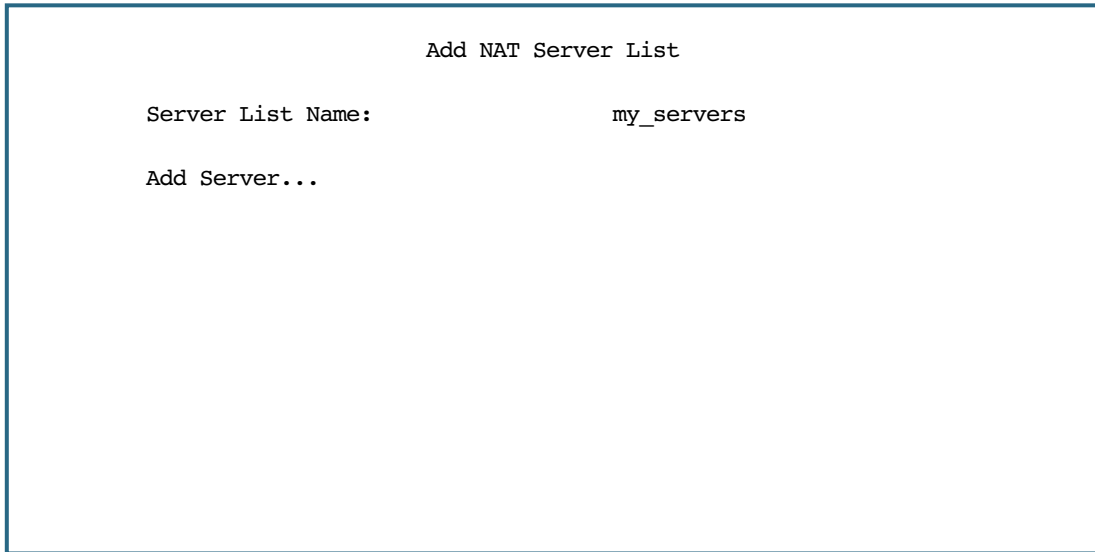
Make any modifications you need and then select **CHANGE NAT MAP** and press Return. Your changes will become effective and you will be returned to the Show/Change NAT Map List screen.

Adding Server Lists

Server lists, also known as Exports, are handled similarly to map lists. If you want to make a particular server's port accessible (and it isn't accessible through other means, such as a static mapping), you must create a server list.

Select **Add Server List** from the Network Address Translation screen.

The Add NAT Server List screen appears.



Add NAT Server List

Server List Name: my_servers

Add Server...

- Select **Server List Name** and type in a descriptive name. A new menu item, **Add Server**, appears.
- Select **Add Server** and press Return. The Add NAT Server screen appears.

Add NAT Server ("my_servers")

Service...

Server Private IP Address:192.168.1.45

Public IP Address:206.1.1.1

ADD NAT SERVERCANCEL

- Select **Service** and press Return. A pop-up menu appears listing a selection of commonly exported services.

Add NAT Server ("my_servers")

Service...

Server Private IP Address:

Public IP Address:

Type	Port(s)
ftp	21
telnet	23
smtp	25
tftp	69
gopher	70
finger	79
www-http	80
pop2	109
pop3	110
snmp	161 - 162
timbuktu	407
pptp	1723
irc	6665 - 6669
Other...	

ADD NAT SERVERCANCEL

- Choose the service you want to export and press Return.
You can choose a preconfigured service from the list, or define your own by selecting **Other**. If you select **Other**, a screen is displayed that allows you to enter the port number range for your customized service.

Other Exported Port	
First Port Number (1..65535):	31337
Last Port Number (1..65535):	31337
<div>OK</div> <div>CANCEL</div>	

- Enter the **First** and **Last Port Number** between ports 1 and 65535. Select **OK** and press Return. You will be returned to the Add NAT Server screen.
 - Enter the **Server Private IP Address** of the server whose service you are exporting.
 Since MultiNAT permits the mapping of multiple private IP addresses to multiple public IP addresses, your ISP or corporate site's Router must be configured such that it knows that your multiple public addresses are accessible via your Router.
 If you want to use static mappings to map internal servers to public addresses, your ISP or corporate site's Router must also be configured for static routes to these public addresses on the Netopia Router.
 - Enter the **Public IP Address** to which you are exporting the service.
- Note:** For PAT map lists and server lists, if you use the Public Address 0.0.0.0, the list will acquire its public IP address from the WAN IP address specified by your WAN IP configuration in the Connection Profile. If that is a static IP address, then the PAT map list and server lists will acquire that address. If it is a negotiated IP address, such as may be assigned via DHCP or PPP, the PAT map list and server lists will acquire that address each time it is negotiated.
- Select **ADD NAT SERVER** and press Return. The server will be added to your server list and you will be returned to the Add NAT Server List screen.

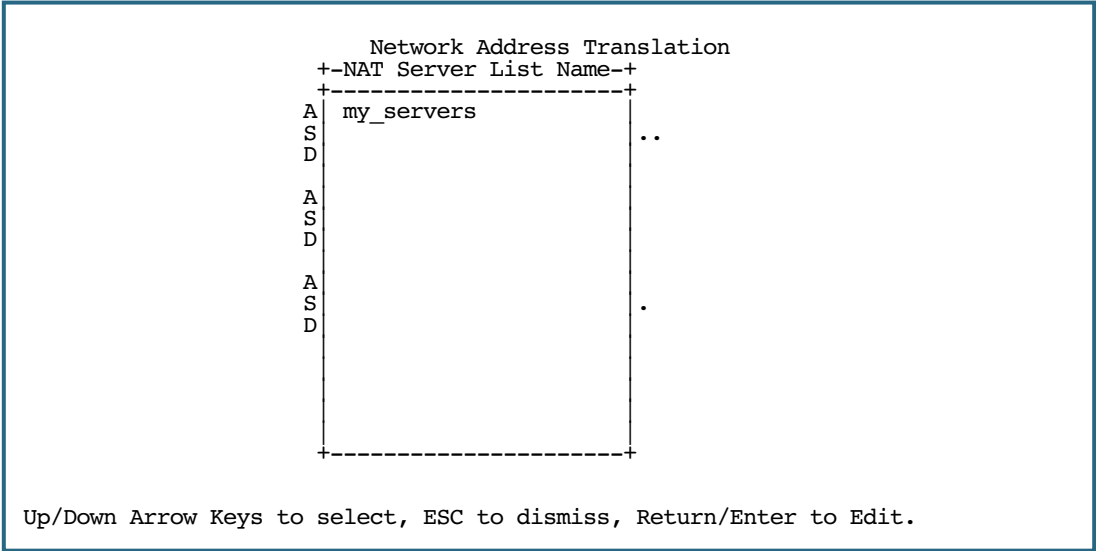
Note: In order to use **CUSeeMe** through the Netopia Router, you must export the ports 7648 and 7649. In MultiNat, you may use a port range export. Without the export, CUSeeMe will fail to work. This is true unless a static mapping is in place for the host using CUSeeMe. In that case no server list entry is necessary.

Modifying server lists

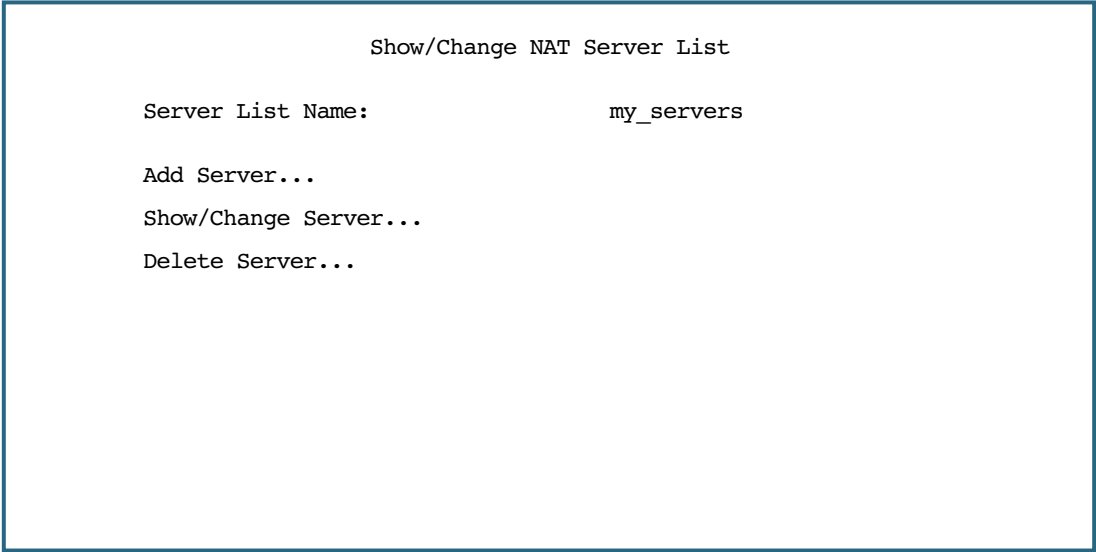
Once a server list exists, you can select it for modification or deletion.

- Select **Show/Change Server List** from the Network Address Translation screen.

- Select the Server List Name you want to modify from the pop-up menu and press Return.



The Show/Change NAT Server List screen appears.



- Selecting **Show/Change Server** or **Delete Server** displays the same pop-up menu.

```

                                Show/Change NAT Server List
          +-Private Address--Public Address---Port-----+
          +-----+
Se  192.168.1.254    206.1.1.6      smtp
    192.168.1.254    206.1.1.5      smtp
    192.168.1.254    206.1.1.4      smtp
Ad  192.168.1.254    206.1.1.3      smtp
    192.168.1.254    206.1.1.1      smtp
Sh
De
          +-----+

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

```

Select any server from the list and press Return. The Change NAT Server screen appears.

```

                                Change NAT Server ("My Exports")

Service...                               smtp
Server Private IP Address:              192.168.1.254
Public IP Address:                      206.1.1.1

CHANGE NAT SERVER                        CANCEL

```

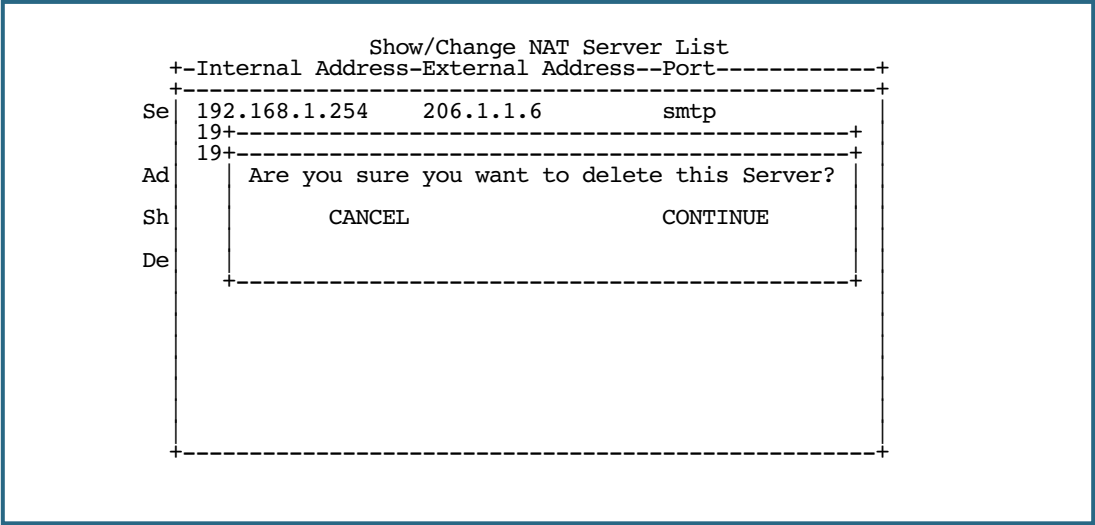
You can make changes to the server's service and port or internal or external address.

Select **CHANGE NAT SERVER** and press Return. Your changes take effect and you are returned to the Show/Change NAT Server List screen.

Deleting a server

To delete a server from the list, select **Delete Server** from the Show/Change NAT Server List menu and press Return.

A pop-up menu lists your configured servers. Select the one you want to delete and press Return. A dialog box asks you to confirm your choice.



Choose **CONTINUE** and press Return. The server is deleted from the list.

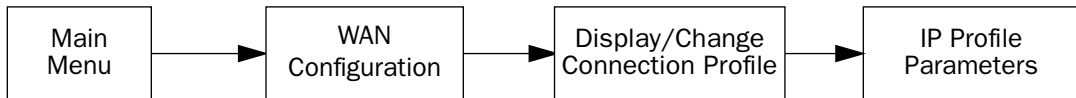
Binding Map Lists and Server Lists

Once you have created your map lists and server lists, for most Netopia Router models you must bind them to a profile, either a Connection Profile or the Default Profile. You do this in one of the following screens:

- the [IP profile parameters](#) screen (see below) of the Connection Profile configuration menu
- the [IP Parameters \(WAN Default Profile\)](#) screen (see [page 3-23](#)) of the Default Profile configuration menu
- the [Binding Map Lists and Server Lists](#) screen (see [page 3-21](#))

IP profile parameters

To bind a map list to a Connection Profile, from the Main Menu go to the WAN Configuration screen then the Display/Change Connection Profile screen. From the pop-up menu list of your Connection Profiles, choose the one you want to bind your map list to. Select **IP Profile Parameters** and press Return.



The IP Profile Parameters screen appears.

IP Profile Parameters

Address Translation Enabled:	Yes
IP Addressing...	Unnumbered
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
Local WAN IP Address:	206.1.1.6
Local WAN IP Mask:	0.0.0.0
Remote IP Address:	127.0.0.2
Remote IP Mask:	255.255.255.255
Filter Set...	Basic Firewall
Remove Filter Set	
RIP Profile Options...	
Configure IP requirements for a remote network connection here.	

- Select **NAT Map List** and press Return. A pop-up menu displays a list of your defined map lists.

IP Profile Parameters

+-NAT Map List Name-+-

Address Trans

IP Addressing

NAT Map List.

NAT Server Li

Local WAN IP

Remote IP Add

Remote IP Mas

Filter Set...

Remove Filter

Receive RIP:

Easy-PAT

my_map

<<None>>

s

mbered

sy PAT

7.0.0.2

5.255.255.255

tBIOS Filter

th

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

- Select the map list you want to bind to this Connection Profile and press Return. The map list you selected will now be bound to this Connection Profile.
- Select **NAT Server List** and press Return. A pop-up menu displays a list of your defined server lists.

IP Profile Parameters

+-NAT Server List Name-+-

Address Trans

IP Addressing

NAT Map List.

NAT Server Li

Local WAN IP

Local WAN IP

Remote IP Add

Remote IP Mas

Filter Set...

Remove Filter

Receive RIP:

Easy-Servers

my_servers

<<None>>

s

mbered

sy PAT

0.0.0

0.0.0

7.0.0.2

5.255.255.255

tBIOS Filter

th

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

- Select the server list you want to bind to this Connection Profile and press Return. The server list you selected will now be bound to this Connection Profile.

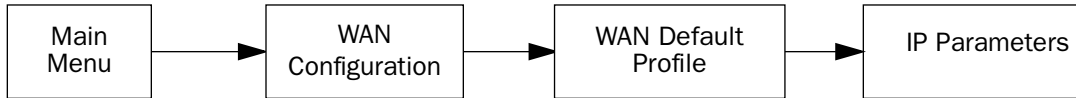
Note: There is no interdependency between NAT and IP Addressing. Also, the Local WAN IP Address and Mask fields' visibility are dependent only on the IP Addressing type.

IP Parameters (WAN Default Profile)

The Netopia Firmware Version 8.4 using RFC 1483 supports a WAN default profile that permits several parameters to be configured without an explicitly configured Connection Profile.

The procedure is similar to the procedure to bind map lists and server lists to a Connection Profile.

From the Main Menu go to the WAN Configuration screen, then the Default Profile screen. Select **IP Parameters** and press Return.



The IP Parameters (Default Profile) screen appears.

IP Parameters (Default Profile)

Address Translation Enabled:	Yes
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
Filter Set (Firewall)...	
Remove Filter Set	
Receive RIP:	Both

Return/Enter to select <among/between> ...

- Toggle **Address Translation Enabled** to Yes.
- Select **NAT Map List** and press Return. A pop-up menu displays a list of your defined map lists.

IP Parameters (Default Profile)

+--NAT Map List Name---+

+-----+
Easy-PAT List
my_map
<<None>>
+-----+

Address Trans

NAT Map List.

NAT Server Li

Filter Set (F

Remove Filter

Receive RIP:

s

th

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

- Select the map list you want to bind to the default profile and press Return. The map list you selected will now be bound to the default profile.
- Select **NAT Server List** and press Return. A pop-up menu displays a list of your defined server lists.

IP Parameters (Default Profile)

+--NAT Server List Name---+

+-----+
Easy-Servers
my_servers
<<None>>
+-----+

Address Trans

NAT Map List.

NAT Server Li

Filter Set (F

Remove Filter

Receive RIP:

s

_first_map

th

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

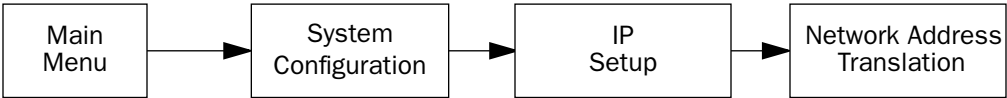
- Select the server list you want to bind to the default profile and press Return. The server list you selected will now be bound to the default profile.

Note: There is no interdependency between NAT and IP Addressing. Also, the Local WAN IP Address and Mask fields' visibility are dependent only on the IP Addressing type.

NAT Associations

Configuration of map and server lists alone is not sufficient to enable NAT for a WAN connection because map and server lists must be linked to a profile that controls the WAN interface. This can be a Connection Profile, a WAN Ethernet interface, a default profile, or a default answer profile. Once you have configured your map and server lists, you may want to reassign them to different interface-controlling profiles, for example, Connection Profiles. To permit easy access to this IP Setup functionality, you can use the NAT Associations screen.

You access the NAT Associations screen from the Network Address Translation screen.



Select **NAT Associations** and press Return. The NAT Associations screen appears.

NAT Associations			
Profile/Interface Name-----	Nat?	Map List Name-----	Server List Name
Default Answer Profile	On	my_first_map	my_servers
Easy Setup Profile	On	Easy-PAT	my_servers
Profile 01	On	my_second_map	my_servers
Profile 02	On	my_first_map	my_server_list
Profile 03	On	<<None>>	<<None>>

- You can toggle **NAT? On** or **Off** for each Profile/Interface name. You do this by navigating to the **NAT?** field associated with each profile using the arrow keys. Toggle NAT on or off by using the Tab key.
- You can reassign any of your map lists or server lists to any of the Profile/Interfaces. You do this by navigating to the **Map List Name** or **Server List Name** field associated with each profile using the arrow keys. Select the item by pressing Return to display a pop-up menu of all of your configured lists.

NAT Associations			
Profile/Interface Name-----	Nat-----	+NAT Map List Name--+	Server List Name
Easy Setup Profile	On	Easy-PAT List	my_servers
Profile 01	On	my_first_map	my_servers
Profile 02	On	my_second_map	my_server_list
Profile 03	On	my_map	<<None>>
Profile 04	On	<<None>>	<<None>>
Default Answer Profile	On	-----	my_servers
Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.			

- Select the list name you want to assign and press Return again. Your selection will then be associated with the corresponding profile or interface.

IP Passthrough

Netopia Firmware Version 8.4 offers an IP passthrough feature. The IP passthrough feature allows for a single PC on the LAN to have the router's public address assigned to it. It also provides PAT (NAPT) via the same public IP address for all other hosts on the private LAN subnet. Using IP passthrough:

- The public WAN IP is used to provide IP address translation for private LAN computers.
- The public WAN IP is assigned and reused on a LAN computer.
- DHCP address serving can automatically serve the WAN IP address to a LAN computer.

When DHCP is used for addressing the designated passthrough PC, the acquired or configured WAN address is passed to DHCP, which will dynamically configure a single-servable-address subnet, and reserve the address for the configured MAC address. This dynamic subnet configuration is based on the local and remote WAN address and subnet mask. If the WAN interface does not have a suitable subnet mask that is usable, for example when using PPP or PPPoE, the DHCP subnet configuration will default to a class C subnet mask.

Globally, only one dynamically-configured DHCP subnet is available. If you configure *multiple* Connection Profiles to use IP Passthrough's DHCP option, when any of these profiles is established, the dynamic DHCP configuration will be overwritten.

In the case of an Ethernet WAN router the IP passthrough configuration is located in the WAN Ethernet Configuration menu. For all other routers, it is located in the Connection Profiles' IP Profile Parameters.

The **WAN Ethernet Configuration** screen, found under the WAN Configuration menu, WAN Setup screen, appears as shown.

WAN Ethernet Configuration

Address Translation Enabled:	Yes
Local WAN IP Address:	0.0.0.0
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
NAT Options...	
Stateful Inspection Enabled:	No
Filter Set...	
Remove Filter Set	
Enable PPP over Ethernet:	Off
WAN Ethernet Speed Setting...	Auto-Negotiation
Wan Ethernet MAC Address:	00:fc:de:fa:dd:02
DHCP Client Mode:	Standards-Based
RIP Options...	

Set up the basic IP attributes of your Ethernet Module in this screen.

The **IP Profile Parameters** screen, found under the WAN Configuration menu, Add/Change Connection Profile screen, appears as shown.

IP Profile Parameters

Address Translation Enabled:	Yes
IP Addressing...	Numbered
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
NAT Options...	
Stateful Inspection Enabled:	No
Local WAN IP Address:	0.0.0.0
Local WAN IP Mask:	0.0.0.0
Filter Set...	
Remove Filter Set	
RIP Profile Options...	

Toggle to Yes if this is a single IP address ISP account.
Configure IP requirements for a remote network connection here.

If you select **NAT Options**, in either case, the NAT Options screen appears.

NAT Options

IP Passthrough Enabled:	No
-------------------------	----

Toggle ON to allow local WAN IP address to be used on LAN in addition to NAT.

If you toggle **IP Passthrough Enabled** to **Yes**, additional field(s) appear.

NAT Options	
IP Passthrough Enabled:	Yes
IP Passthrough DHCP Enabled:	Yes
IP Passthrough DHCP MAC address:	00-00-00-00-00-00

Enter MAC addr. of IP passthrough host, or zeroes for first come first serve.

Toggling **IP Passthrough DHCP Enabled** to **Yes** displays the **IP Passthrough DHCP MAC address** field. This is an editable field in which you can enter the MAC (hardware) address of the designated PC be used as the DHCP Client Identifier for dynamic address reservation. The MAC address must be six colon-delimited or dash-delimited sets of hex digits ('0' – 'FF').

First Come First Serve Mode

Netopia Firmware Version 8.4 IP Passthrough allows a *first come first serve* mode.

NAT Options defaults to an all-zeroes MAC address.

If you leave the default all-zeroes MAC address, the Router will select the next DHCP client that initiates a DHCP lease request or renewal to be the IP passthrough host. When the WAN comes up, or if it is already up, the Router will serve this client the IP passthrough/WAN address. When this client's lease ends, the IP passthrough address becomes available for the next client to initiate a DHCP transaction. The next client will get the IP passthrough address. Note that there is no way to control which PC has the IP passthrough address without releasing all other DHCP leases on the LAN.

Note: If you specify a non-zeroes MAC address, the DHCP Client Identifier must be in the format specified above. Macintosh computers allow the DHCP Client Identifier to be entered as a name or text, however Netopia routers accept only strict (binary/hex) MAC address format. Macintosh computers display their strict MAC addresses in the TCP/IP Control Panel (Classic MacOS) or the Network Preference Pane of System Preferences (Mac OS X).

Once configured, the passthrough host's DHCP leases will be shortened to two minutes. This allows for timely updates of the host's IP address, which will be a private IP address *before* the WAN connection is established. *After* the WAN connection is established and has an address, the passthrough host can renew its DHCP address binding to acquire the WAN IP address.

A restriction

Since both the router and the passthrough host will use same IP address, new sessions that conflict with existing sessions will be rejected by the router. For example, suppose you are a teleworker using an IPSec tunnel from the router *and* from the passthrough host. Both tunnels go to the same remote endpoint, such as the VPN access concentrator at your employer's office. In this case, the first one to start the IPSec traffic will be allowed; the second one – since, from the WAN it's indistinguishable – will fail.

MultiNAT Configuration Example

To help you understand a typical MultiNAT configuration, this section describes an example of the type of configuration you may want to implement on your site. The values shown are for example purposes only. *Make your own appropriate substitutions.*

A typical DSL service from an ISP might include five user addresses. Without PAT, you might be able to attach only five IP hosts. Using simple 1-to-many PAT you can connect more than five devices, but use only one of your addresses. Using multiNAT you can make full use of the address range. The example assumes the following range of addresses offered by a typical ISP:

Local WAN IP address:	206.1.1.6
Local WAN subnet mask:	255.255.255.248
Remote IP address:	206.1.1.254
Default gateway:	206.1.1.254

Public IP addresses assigned by the ISP are 206.1.1.1 through 206.1.1.6 (255.255.255.248 subnet mask).

Your internal devices have IP addresses of 192.168.1.1 through 192.168.1.254 (255.255.255.0 subnet mask).

Netopia Router's address is:	192.168.1.1
Web server's address is:	192.168.1.253
Mail server's address is:	192.168.1.254
FTP server's address is:	192.168.1.253

In this example you will statically map the first five public IP addresses (206.1.1.1 - 206.1.1.5) to the first five corresponding private IP addresses (192.168.1.1 - 192.168.1.5). You will use these 1-to-1 mapped addresses to give your servers “real” addresses. You will then map 206.1.1.6 to the remaining private IP addresses (192.168.1.6 - 192.168.1.254) using PAT.

The configuration process is as follows:

From the Main Menu go to the Easy Setup and then the Connection Profile screen.



Enter your ISP-supplied values as shown below.

Connection Profile 1: Easy Setup Profile

Connection Profile Name:

Easy Setup Profile

Address Translation Enabled:

Yes

IP Addressing...

Numbered

Local WAN IP Address:

206.1.1.6

Local WAN IP Mask:

255.255.255.248

PREVIOUS SCREEN

NEXT SCREEN

Enter a subnet mask in decimal and dot form (xxx.xxx.xxx.xxx).

Enter basic information about your WAN connection with this screen.

Select **NEXT SCREEN** and press Return.

Your IP values are shown here.

IP Easy Setup

Ethernet IP Address:

192.168.1.1

Ethernet Subnet Mask:

255.255.255.0

Domain Name:

ISP.net

Primary Domain Name Server:

173.166.101.1

Secondary Domain Name Server:

173.166.102.1

Default IP Gateway:

206.1.1.254

IP Address Serving:

On

Number of Client IP Addresses:

20

1st Client Address:

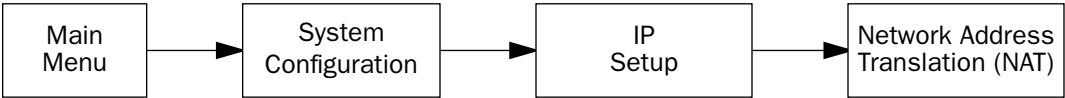
192.168.1.2

PREVIOUS SCREEN

NEXT SCREEN

Set up the basic IP & IPX attributes of your Netopia in this screen.

Then navigate to the Network Address Translation (NAT) screen.



Select **Show/Change Public Range**, then **Easy-PAT Range**, and press Return. Enter the value your ISP assigned for your public address (206.1.1.6, in this example). Toggle **Type** to pat. Your public address is then mapped to the remaining private IP addresses using PAT. (If you were not using the Easy-PAT Range and Easy-PAT List that are created by default by using Easy Setup, you would have to *define* a public range and map list. For the purpose of this example you can just *alter* this range and list.)

Change NAT Public Range	
Range Name:	Easy-PAT Range
Type...	pat
Public Address:	206.1.1.6
First Public Port:	49152
Last Public Port:	65535
CHANGE NAT PUBLIC RANGE	CANCEL

Select **CHANGE NAT PUBLIC RANGE** and press Return. This returns you to the Network Address Translation screen.

Select **Add Public Range** and press Return. Type a name for this static range, as shown below. Enter the first and last public addresses your ISP assigned in their respective fields as shown. The first five public IP addresses (206.1.1.1 - 206.1.1.5, in this example) are statically mapped to the first five corresponding private IP addresses (192.168.1.1 - 192.168.1.5).

Add NAT Public Range	
Range Name:	Static Range
Type...	static
First Public Address:	206.1.1.1
Last Public Address:	206.1.1.5
ADD NAT PUBLIC RANGE	CANCEL

Return/Enter to commit changes.

Select **ADD NAT PUBLIC RANGE** and press Return. You are returned to the Network Address Translation screen.

Next, select **Show/Change Map List** and choose **Easy-PAT List**. Select **Add Map**. The **Add NAT Map** screen appears. (Now the name *Easy-PAT List* is a misnomer since it has a static map included in its list.) Enter in 192.168.1.1 for the **First Private Address** and 192.168.1.5 for the **Last Private Address**.

Add NAT Map ("Easy-PAT List")

First Private Address:

192.168.1.1

Last Private Address:

192.168.1.5

Use NAT Public Range...

ADD NAT MAP

CANCEL

Select **Use NAT Public Range** and from the pop-up menu choose **Static Range**. Select **ADD NAT MAP** and press Return.

This will statically map the first five public IP addresses to the first five corresponding private IP addresses and will map 206.1.1.6 to the remaining private IP addresses using PAT.

Notes on the example

The Easy-Map List and the Easy-PAT List are attached to any new Connection Profile by default. If you want to use this NAT configuration on a previously defined Connection Profile then you need to *bind* the Map List to the profile. You do this through either the NAT Associations screen or the profile's configuration screens.

The PAT part of this example setup will allow any user on the Netopia Router's LAN with an IP address in the range of 192.168.1.6 through 192.168.1.254 to *initiate* traffic flow to the outside world (for example, the Internet). No one on the Internet would be able to initiate a conversation with them.

The Static mapping part of this example will allow any of the machines in the range of addresses from 192.168.1.1 through 192.168.1.5 to communicate with the outside world as if they were at the addresses 206.1.1.1 through 206.1.1.5, respectively. It also allows any machine on the Internet to access any service (port) on any of these five machines.

You may decide this poses a security risk. You may decide that anyone can have complete access to your FTP server, but not to your Router, and only limited access to the desired services (ports) on the Web and Mail servers.

To make these changes, first limit the range of remapped addresses on the Static Map and then edit the default server list called Easy-Servers.

- First, navigate to the **Show/Change Map List** screen, select **Easy-PAT List** and then **Show/Change Maps**. Choose the **Static Map** you created and change the **First Private Address** from 192.168.1.1 to 192.168.1.4. Now the Router, Web, and Mail servers' IP addresses are no longer included in the range of static mappings and are therefore no longer accessible to the outside world. Users on the Internet will not be able to Telnet, Web, SNMP, or ping to them. It is best also to navigate to the public range screen and change the **Static Range** to go from 206.1.1.5.
- Next, navigate to **Show/Change Server List** and select **Easy-Servers** and then **Add Server**. You should export both the Web (www-http) and Mail (smtp) ports to one of the now free public addresses. Select **Service...** and from the resulting pop-up menu select **www-http**. In the resulting screen enter your Web server's address, 192.168.1.2, and the public address, for example, 206.1.1.2, and then select **ADD NAT SERVER**. Now return to **Add Server**, choose the **smtp** port and enter 192.168.1.3, your Mail server's IP address for the **Server Private IP Address**. You can decide if you want to present both your Web and Mail services as being on the same public address, 206.1.1.2, or if you prefer to have your Mail server appear to be at a different IP address, 206.1.1.3. For the sake of this example, alias both services to 206.1.1.2.

Now, as before, the PAT configuration will allow any user on the Netopia Router's LAN with an IP address in the range of 192.168.1.6 through 192.168.1.254 to initiate traffic flow to the Internet. Someone at the FTP server can access the Internet and the Internet can access all services of the FTP machine as if it were at 206.1.1.5. The Router cannot directly communicate with the outside world. The only communication between the Web server and the Internet is through port 80, the Web port, as if the server were located on a machine at IP address 206.1.1.2. Similarly, the only communication with the Mail server is through port 25, the SMTP port, as if it were located at IP address 206.1.1.2

Chapter 4

Virtual Private Networks (VPNs)

The Netopia Firmware Version 8.4 offers IPsec, PPTP, and ATMP tunneling support for Virtual Private Networks (VPN).

The following topics are covered in this chapter:

- ["Overview" on page 4-1](#)
- ["About PPTP Tunnels" on page 4-4](#)
- ["About IPsec Tunnels" on page 4-7](#)
- ["About L2TP Tunnels" on page 4-8](#)
- ["About GRE Tunnels" on page 4-11](#)
- ["About ATMP Tunnels" on page 4-15](#)
- ["Encryption Support" on page 4-17](#)
- ["ATMP/PPTP Default Profile" on page 4-18](#)
- ["VPN QuickView" on page 4-20](#)
- ["Dial-Up Networking for VPN" on page 4-21](#)
- ["Allowing VPNs through a Firewall" on page 4-24](#)
- ["Windows Networking Broadcasts" on page 4-31](#)

Overview

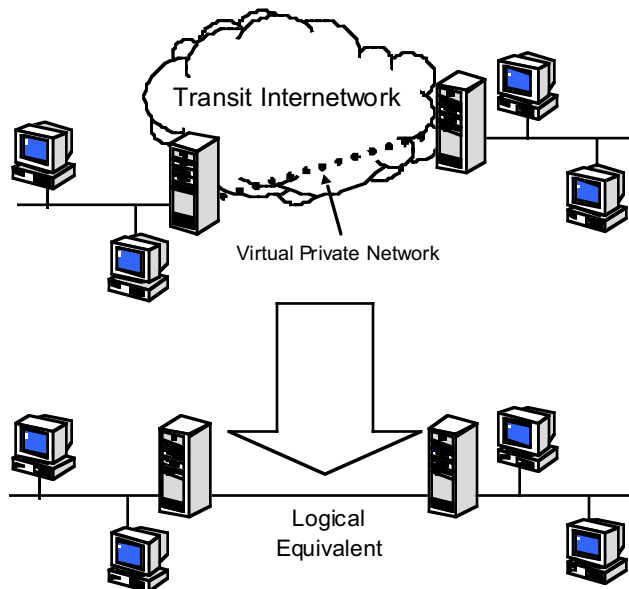
When you make a long distance telephone call from your home to a relative far away, you are creating a private network. You can hold a conversation, and exchange information about the happenings on opposite sides of the state, or the continent, that you are mutually interested in. When your next door neighbor picks up the phone to call her daughter at college, at the same time you are talking to your relatives, your calls don't overlap, but each is separate and private. Neither house has a direct wire to the places they call. Both share the same lines on the telephone poles (or underground) on the street.

These calls are *virtual private networks*. *Virtual*, because they appear to be direct connections between the calling and answering parties, even though they travel over the public wires and switches of the phone company; *private*, because neither pair of calling and answering parties interacts with the other; and *networks*, because they exchange information.

Computers can do the same thing; it's called Virtual Private Networks (VPNs). Equipped with a Netopia Router, a single computer or private network (LAN) can establish a private connection with another computer or private network over the public network (Internet).

Netopia Firmware Version 8.4 can be used in VPNs either to initiate the connection or to answer it. When used in this way, the Routers are said to be *tunnelling* through the public network (Internet). The advantages are that, like your long distance phone call, you don't need a direct line between one computer or LAN and the other, but use the local connections, making it much cheaper; and the information you exchange through your tunnel is private and secure.

Tunneling is a process of creating a private path between a remote user or private network and another private network over some intermediate network, such as the IP-based Internet. A VPN allows remote offices or employees access to your internal business LAN through means of encryption allowing the use of the public Internet to look “virtually” like a private secure network. When two networks communicate with each other through a network based on the Internet Protocol, they are said to be *tunneling* through the IP network.



Unlike the phone company, private and public computer networks can use more than one protocol to carry your information over the wires. Several such protocols are in common use for tunnelling, Point-to-Point Tunnelling Protocol (PPTP), IP Security (IPsec), Layer 2 Transport Protocol (L2TP), Generic Routing Encapsulation (GRE), and Ascend Tunnel Management Protocol (ATMP). The Netopia Router can use any of these.

- Point-to-Point Tunneling Protocol (PPTP) is an extension of Point-to-Point Protocol (PPP) and uses a client and server model. Netopia's PPTP implementation is compatible with Microsoft's and can function as either the client (PAC) or the server (PNS). As a client, a Netopia Router can provide all users on a LAN with secure access over the Internet to the resources of another LAN by setting up a tunnel with a Windows NT server running Remote Access Services (RAS) or with another Netopia Router. As a server, a Netopia Router can provide remote users a secure connection to the resources of the LAN over a dial-up, cable, DSL, or any other type of Internet access. Because PPTP can create a VPN tunnel using the Dial-Up Networking (DUN) (see ["Dial-Up Networking for VPN" on page 4-21](#)) utility built into Windows 95, 98, or NT, no additional client software is required.
- IPsec stands for IP Security, a set of protocols that supports secure exchange of IP packets at the IP layer. IPsec is deployed widely to implement Virtual Private Networks (VPNs). IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but

leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet. The Netopia Firmware Version 8.4 supports the more secure Tunnel mode.

DES stands for Data Encryption Standard, a popular symmetric-key encryption method. DES uses a 56-bit key. The Netopia Firmware Version 8.4 offers IPsec DES encryption over the VPN tunnel.

- Ascend Tunnel Management Protocol (ATMP) is the protocol that is implemented in many Ascend gateways. ATMP is a simple protocol for connecting nodes and/or networks together over the Internet via a tunnel. ATMP encapsulates IP or other user data without PPP headers within General Routing Encapsulation (GRE) protocol over IP. ATMP is more efficient than PPTP for network-to-network tunnels.

When used to initiate the tunnelled connection, the Router is called a *PPTP Access Concentrator* (PAC, in PPTP language), or a *foreign agent* (in ATMP language). When used to answer the tunnelled connection, the Netopia Router is called a *PPTP Network Server* (PNS, in PPTP language) or a *home agent* (in ATMP language).

In either case, the Netopia Router wraps, or encapsulates, information that one end of the tunnel exchanges with the other, in a wrapper called General Routing Encapsulation (GRE), at one end of the tunnel, and unwraps, or decapsulates, it at the other end.

Configuring the Netopia Router for use with the different protocols is done through the Telnet-based menu screens. Each type is described in its own section:

- ["About PPTP Tunnels" on page 4-4](#)
- ["About IPsec Tunnels" on page 4-7](#)
- ["About L2TP Tunnels" on page 4-8](#)
- ["About GRE Tunnels" on page 4-11](#)
- ["About ATMP Tunnels" on page 4-15](#)

Your configuration depends on which protocol you (and the gateway at the other end of your tunnel) will use, and whether or not you will be using VPN client software in a standalone remote connection.

Note: You must choose which protocol you will be using, since you cannot both export PPTP and use ATMP, or vice versa, at the same time.

Having both an ATMP tunnel and a PPTP export is not possible because functions require GRE and the Router's PPTP export/server does not distinguish the GRE packets it forwards. Since it processes all of them, ATMP tunneling is impaired. For example, you cannot run an ATMP tunnel between two gateways and also have PPTP exported on one side.

Summary

A Virtual Private Network (VPN) connects the components of one network over another network. VPNs accomplish this by allowing you to *tunnel* through the Internet or another public network in a manner that provides the same security and features formerly available only in private networks.

VPNs allow networks to communicate across an IP network. Your local networks (connected to the Netopia Router) can exchange data with remote networks that are also connected to a VPN-capable gateway.

This feature provides individuals at home, on the road, or in branch offices with a cost-effective and secure way to access resources on remote LANs connected to the Internet with Netopia Routers.

About PPTP Tunnels

To set up a PPTP tunnel, you create a Connection Profile including the IP address and other relevant information for the remote PPTP partner. You use the same procedure to initiate a PPTP tunnel that terminates at a remote PPTP server or to terminate a tunnel initiated by a remote PPTP client.

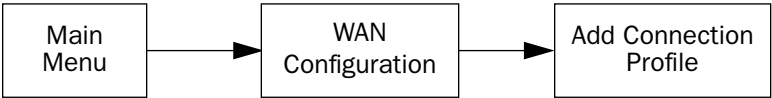
PPTP configuration

To set up the Router as a PPTP Network Server (PNS) capable of answering PPTP tunnel requests you must also configure the VPN Default Answer Profile. See ["ATMP/PPTP Default Profile" on page 4-18](#) for more information.

PPTP is a Datalink Encapsulation option in Connection Profiles. It is not an option in device or link configuration screens, as PPTP is not a native encapsulation. Consequently, the Easy Setup Profile does not offer PPTP datalink encapsulation. See the ["Creating a New Connection Profile" on page 2-9](#) for information on creating Connection Profiles.

Channel 4 (and higher) events, such as connections and disconnections, reported in the WAN Event Histories are VPN tunnel events.

To define a PPTP tunnel, navigate to the Add Connection Profile menu from the Main Menu.



Add Connection Profile

Profile Name:	Profile 2
Profile Enabled:	+-----+
Encapsulation Type...	+-----+
Underlying Encapsulation...	PPP
Encapsulation Options...	ATMP
	PPTP
	IPsec
	L2TP
	GRE
IP Profile Parameters...	+-----+
Interface Group...	Primary
COMMIT	CANCEL

When you define a Connection Profile as using PPTP by selecting PPTP as the datalink encapsulation method, and then select **Data Link Options**, the PPTP Tunnel Options screen appears.

PPTP Tunnel Options	
PPTP Partner IP Address:	173.167.8.134
Tunnel Via Gateway:	0.0.0.0
Authentication...	CHAP
Data Compression...	None
Send Host name:	tony
Send Password:	*****
Receive Host name:	kimba
Receive Password:	*****
Initiate Connections:	Yes
On Demand:	Yes
Optional Windows NT Domain Name:	
Idle Timeout (seconds):	300

- Enter the **PPTP Partner IP Address**. This specifies the address of the other end of the tunnel.
If you do not specify the PPTP Partner IP Address the Router cannot initiate tunnels, i.e., act as a PPTP Access Concentrator (PAC) for this profile. It can only accept tunnel requests as a PPTP Network Server (PNS).
- If you specify the PPTP Partner IP Address, and the address is in the same subnet as the Remote IP Address you specified in the IP Profile Parameters, the **Tunnel Via Gateway** option becomes visible. You can enter the address by which the Router partner is reached.
If you do not specify the PPTP Partner IP Address, the Router will use the default gateway to reach the partner and the **Tunnel Via Gateway** field is hidden. If the partner should be reached via an alternate port (i.e. the LAN instead of the WAN), the **Tunnel Via Gateway** field allows this path to be resolved.
- From the pop-up menu select an **Authentication** protocol for the PPP connection. Options are PAP, CHAP, or MS-CHAP. The default is PAP. The authentication protocol must be the same on both ends of the tunnel.
- You can specify a **Data Compression** algorithm, either None or Standard LZS, for the PPTP connection.
Note: When the Authentication protocol is MS-CHAP, compression is set to None, and the **Data Compression** option is hidden.
- When the authentication protocol is MS-CHAP, you can specify a **Data Encryption** algorithm for the PPTP connection. Available options are MPPE and None (the default). For other authentication protocols, this option is hidden. When MPPE is negotiated, the WAN Event History reports that it is negotiated as a CCP (compression) type. This is because the MPPE protocol uses a compression engine, even though it is not itself a compression protocol.

Note: Netopia Firmware Version 8.4 supports 128-bit (“strong”) encryption. Unlike MS-CHAP version 1, which supports one-way authentication, MS-CHAP version 2 supports mutual authentication between connected gateways and is incompatible with MS-CHAP version 1 (MS-CHAP-V1). When you choose MS-CHAP as the authentication method for the PPTP tunnel, the Netopia Router will start negotiating MS-CHAP-V2. If the gateway you are connecting to does not support MS-CHAP-V2, it will fall back to MS-CHAP-V1, or, if the gateway you are connecting to does not support MPPE at all, the PPP session will be dropped.

- You can specify a **Send Host Name** which is used with Send Secret for authenticating with a remote PNS when the profile is used for initiating a tunnel connection.
- You must specify a **Send Password** (the CHAP and MS-CHAP term for password), used for authenticating the tunnel when initiating a tunnel connection.
- You can specify a **Receive Host Name** which is used with the Receive Secret for authenticating a remote PPTP client.
- You must specify a **Receive Password**, used for authenticating the remote PPTP client.
- You can specify that this Router will **Initiate Connections** (acting as a PAC) or only answer them (acting as a PNS).
- Tunnels are normally initiated **On Demand**; however, you can disable this feature. When disabled, the tunnel must be manually established or may be scheduled using the scheduled connections feature. See ["Scheduled Connections" on page 2-15](#).
- Some networks that use Microsoft Windows NT PPTP Network Servers require additional authentication information, called *Windows NT Domain Name*, when answering PPTP tunnel connection requests. Not all Windows NT installations require this information, since not all such installations use this authentication feature. The Windows NT Domain Name is not the same as the Internet domain name, but is the name of a group of servers that share common security policy and user account databases. Your PPTP tunnel partner's administrator will supply this Windows NT Domain Name if it is required. If you configure your Router to initiate PPTP tunnel connections by toggling **Initiate Connections** to **Yes**, the **Optional Windows NT Domain Name** field appears. Enter the domain name your network administrator has supplied.
- You can specify the **Idle Timeout**, an inactivity timer, whose expiration will terminate the tunnel. A value of zero disables the timer. Because tunnels are subject to abrupt termination when the underlying datalink is torn down, use of the Idle Timeout is strongly encouraged.
- Return to the Connection Profile screen by pressing Escape.
- Select **IP Profile Parameters** and press Return.

The IP Profile Parameters screen appears.

IP Profile Parameters

Address Translation Enabled:	Yes
NAT Map List...	Easy-PAT
NAT Server List...	Easy-Servers
Local WAN IP Address:	0.0.0.0
Remote IP Address:	173.167.8.10
Remote IP Mask:	255.255.0.0
Filter Set...	
Remove Filter Set	
RIP Profile Options...	

- Enter the **Remote IP Address** and **Remote IP Mask** for the host to which you want to tunnel.

About IPsec Tunnels

IPsec stands for IP Security, a set of protocols that supports secure exchange of IP packets at the IP layer. IPsec is deployed widely to implement Virtual Private Networks (VPNs). See ["Overview" on page 4-1](#) for more information.

IPsec supports two encryption modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. The more secure Tunnel mode encrypts both the header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet. Netopia Routers support the more secure Tunnel mode.

Netopia Firmware Version 8.4 offers IPsec 3DES encryption over the VPN tunnel. *DES* stands for Data Encryption Standard, a popular symmetric-key encryption method. DES uses a 56-bit key. Netopia Routers offer IPsec 3DES (triple DES) encryption as a standard option. Some models support built-in hardware acceleration of 3DES encryption at line speeds.

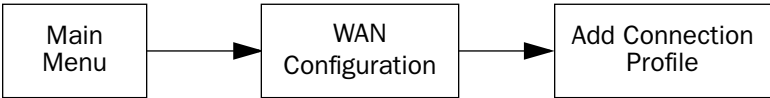
Internet Key Exchange (IKE) is an authentication and encryption key management protocol used in conjunction with the IPsec standard. IPsec key management offers a wide variety of options which are explained in [Chapter 5, "Internet Key Exchange \(IKE\) IPsec Key Management for VPNs."](#)

About L2TP Tunnels

L2TP stands for Layer 2 Tunnelling Protocol, an extension to the PPP protocol. L2TP combines features of two other tunneling protocols: PPTP and L2F. Like PPTP, L2TP is a Datalink Encapsulation option in Connection Profiles. It is not an option in device or link configuration screens, as L2TP is not a native encapsulation. Consequently, the Easy Setup Profile does not offer L2TP datalink encapsulation. See the ["Creating a New Connection Profile" on page 2-9](#) for information on creating Connection Profiles.

L2TP configuration

To define an L2TP tunnel, navigate to the Add Connection Profile menu from the Main Menu.



Add Connection Profile

Profile Name:

Profile Enabled:

Encapsulation Type...

Encapsulation Options...

IP Profile Parameters...

Profile 1

+

-----+

+

-----+

PPP

ATMP

PPTP

IPsec

L2TP

+

-----+

COMMIT

CANCEL

When you define a Connection Profile as using L2TP by selecting L2TP as the datalink encapsulation method, and then select **Encapsulation Options**, the L2TP Tunnel Options screen appears.

L2TP Tunnel Options	
L2TP Partner IP Address:	0.0.0.0
L2TP Tunnel Authentication:	No
PPP Authentication:	PAP
Data Compression...	Standard LZS
Send Host Name:	
Send Password:	
Receive Host Name:	
Receive Password:	
Initiate Connections:	Yes
On Demand:	Yes
Idle Timeout (seconds):	300

Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).

- Enter the **L2TP Partner IP Address**. This specifies the address of the other end of the tunnel.
If you do not specify the L2TP Partner IP Address the Router cannot initiate tunnels.
- If you specify the L2TP Partner IP Address, and the address is in the same subnet as the Remote IP Address you specified in the IP Profile Parameters, the **Tunnel Via Gateway** option becomes visible. You can enter the address by which the Router partner is reached.
If you do not specify the L2TP Partner IP Address, the Router will use the default gateway to reach the partner and the **Tunnel Via Gateway** field is hidden. If the partner should be reached via an alternate port (i.e. the LAN instead of the WAN), the **Tunnel Via Gateway** field allows this path to be resolved.
- Toggle **L2TP Tunnel Authentication** to No or Yes.
If you set authentication on the tunnel, an editable **Pass-phrase** field appears where you can specify a password between eight and 15 characters long.
- From the pop-up menu select a **PPP Authentication** protocol for the PPP connection. Options are PAP, or CHAP. The default is PAP. The authentication protocol must be the same on both ends of the tunnel.
- You can specify a **Data Compression** algorithm, either None or Standard LZS, for the L2TP connection.
- You can specify a **Send Host Name** which is used with Send Secret for authenticating with a remote PNS when the profile is used for initiating a tunnel connection.
- You must specify a **Send Password** (or **Secret**, the CHAP term for password), used for authenticating the tunnel when initiating a tunnel connection.
- You can specify a **Receive Host Name** which is used with the Receive Secret for authenticating a remote L2TP client.
- You must specify a **Receive Password** (or CHAP **Secret**), used for authenticating the remote L2TP client.

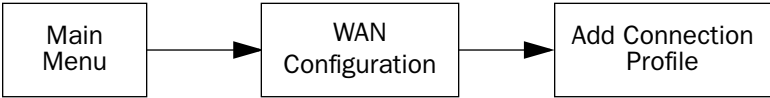
- You can specify that this Router will **Initiate Connections** (acting as a PAC) or only answer them (acting as a PNS).
- Tunnels are normally initiated **On Demand**; however, you can disable this feature. When disabled, the tunnel must be manually established or may be scheduled using the scheduled connections feature. See ["Scheduled Connections" on page 2-15](#).
- You can specify the **Idle Timeout** (in seconds), an inactivity timer, whose expiration will terminate the tunnel. A value of zero disables the timer. Because tunnels are subject to abrupt termination when the underlying datalink is torn down, use of the Idle Timeout is strongly encouraged.
- Return to the Connection Profile screen by pressing Escape.
- Select **IP Profile Parameters** and press Return.
- In the **Profile Parameters** screen, enter the **Remote IP Address** and **Remote IP Mask** for the host to which you want to tunnel. Press Escape to return to the Connection Profile screen. Select **COMMIT** and press Return. The tunnel Connection Profile will be activated.

About GRE Tunnels

Generic Routing Encapsulation (GRE) protocol is another form of tunneling that Netopia routers support. A GRE tunnel is brought up when a valid GRE profile is installed, and brought down when the profile is disabled, or deleted.

GRE tunnels are not *connection-based*, but rather are installed and simply wait for GRE packets. There is no special startup initiation as with PPPoE or PPTP. GRE is best adapted to simple routing and/or tunneling, and is not for use with any sensitive data. GRE offers no encryption; and authentication of data integrity is limited to checksum verification, if enabled.

To set up a GRE tunnel, you create a Connection Profile including the IP address and other relevant information for the remote partner.



Add Connection Profile

Profile Name:	Profile 2
Profile Enabled:	<div>+-----+</div>
Encapsulation Type...	<div>+-----+</div>
Underlying Encapsulation...	PPP
	ATMP
	PPTP
Encapsulation Options...	IPsec
	L2TP
	GRE
IP Profile Parameters...	<div>+-----+</div>
Interface Group...	Primary
COMMIT	CANCEL

When you define a Connection Profile as using GRE by selecting **GRE** as the Encapsulation Type, and then select **Encapsulation Options**, the GRE Tunnel Options screen appears.

GRE Tunnel Options

GRE Partner IP Address:	173.167.8.134
Send Checksums:	No
Sequence Datagrams:	No
Key:	0

Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).

- Enter a **GRE Partner IP Address** in standard dotted-quad format to specify the address of the other end of the tunnel.
 - You can optionally toggle **Send Checksums** to **Yes** to verify that no data corruption or loss is incurred in transmission. Ordinarily, it is not necessary to send checksums, and you can leave the default No.
 - **Sequence Datagrams** can also be left at the default No, unless you are otherwise instructed. Datagram sequencing is mainly needed if compression is being used.
 - You can enter a 32- bit **Key** of up to 10-digits (numbers only). The receiver can use this key to identify the source of the packet. The key is a way to match a packet to a tunnel connection.
- If you choose to enter a key, be sure that both tunnel endpoints' configurations have matching keys.
- If you enter a zero (0), the key field is disabled.
 - Return to the Add Connection Profile screen by pressing Escape.
 - Select **IP Profile Parameters** and press Return.

The IP Profile Parameters screen appears.

IP Profile Parameters

Address Translation Enabled:	No
IP Addressing...	Unnumbered

Remote IP Address:	173.167.8.134
Remote IP Mask:	255.255.0.0
Filter Set...	
Remove Filter Set	

RIP Profile Options...

Toggle to Yes if this is a single IP address ISP account.
Configure IP requirements for a remote network connection here.

- Enter the **Remote IP Address** and **Remote IP Mask** for the host to which you want to tunnel.
- Press Escape to return to the Add Connection profile screen, select COMMIT and press Return. Your GRE Connection Profile will be enabled.

VPN force-all

GRE tunnelling supports “VPN force-all,” which forces all traffic coming from the LAN onto the GRE tunnel. You accomplish this by setting the default route to go through the GRE tunnel. A secondary host route where all tunneled GRE packets route to the actual WAN interface can be configured as a static route when required.

The following table outlines various force-all configurations for different networking scenarios; all other options can safely use their default values:

	Easy Setup	System Configuration Menu	GRE Profile Encapsulation Menu	GRE Profile IP Parameters Menu
Static WAN IP	IP = <i>some_IP_address</i> Mask = <i>some_IP_mask</i> Data Link Encapsulation = 1483, 1490, HDLC, PPP	IP Default Gateway = 127.0.0.2 Gateway Static Route: Destination Network = GRE <i>Remote_Tunnel_End_Point</i> Destination Netmask = <i>Remote_Tunnel_End_Point_netmask</i> Next Gateway = <i>local_WAN_IP</i>	Remote Tunnel End Point = <i>peer_tunnel_IP_address</i>	Remote Member IP = 127.0.0.2 Remote Member Mask cannot be 255.255.255.255
Dynamic WAN IP	IP = 0.0.0.0 Mask = 0.0.0.0	IP Default Gateway = 127.0.0.2 Gateway static route is recommended	see above	see above
Static PPPoE	Remote IP = <i>some_IP_address</i> Remote Mask = <i>some_IP_mask</i>	see above	see above	see above
Auto PPPoE	Remote IP = 127.0.0.2 Remote Mask = 255.255.255.255	IP Default Gateway = 127.0.0.3	see above	Remote Member IP = 127.0.0.3 Remote Member Mask cannot be 255.255.255.255

Note: A GRE tunnel cannot transmit RIP routes over a force-all tunnel, or with a remote member IP with a host part of all zeros.

When you define a Connection Profile as using ATMP by selecting ATMP as the datalink encapsulation method, and then select **Data Link Options**, the ATMP Tunnel Options screen appears.

ATMP Tunnel Options

ATMP Partner IP Address:	173.167.8.134
Tunnel Via Gateway:	0.0.0.0
Network Name:	sam.net
Password:	****
Data Encryption...	DES
Key String:	
Initiate Connections:	Yes
On Demand:	Yes
Idle Timeout (seconds):	300

Note: An ATMP tunnel cannot be assigned a dynamic IP address by the remote server, as in a PPP connection. When you define an ATMP tunnel profile, the Local WAN IP Address, assigned in the IP Profile Parameters screen, must be the true IP address, not 0.0.0.0, if NAT is enabled.

- **ATMP Partner IP Address** specifies the address of the other end of the tunnel. When unspecified, the Router can not initiate tunnels (i.e., act as a foreign agent) for this profile; it can only accept tunnel requests as a home agent.
- When you specify the ATMP Partner IP Address, and the address is in the same subnet as the Remote IP Address you specified in the IP Profile Parameters, you can specify the route (**Tunnel Via Gateway**) by which the Router partner is reached. If you do not specify the ATMP Partner IP Address, the Router will use the default gateway to reach the partner and the **Tunnel Via Gateway** field is hidden. If the partner should be reached via an alternate port (i.e., the LAN instead of the WAN), the **Tunnel Via Gateway** field allows this path to be resolved.
- You can specify a **Network Name**. When the tunnel partner is another Netopia Router, this name may be used to match against a Connection Profile. When the partner is an Ascend gateway in Gateway mode, then **Network Name** is used by the Ascend gateway to match a gateway profile. When the partner is an Ascend gateway in Gateway mode, leave this field blank.
- You must specify a **Password**, used for authenticating the tunnel.
Note: The Password entry will be the same for both ends of the tunnel.
- For Netopia-to-Netopia connections only, you can specify a **Data Encryption** algorithm for the ATMP connection from the pop-up menu, either DES or None. None is the default.
Note: Ascend does not support DES encryption for ATMP tunnels.
- You must specify a **Key String** of up to (and including) 20 characters when DES is selected. When encryption is None, this field is invisible.

- You can specify that this Router will **Initiate Connections**, acting as a foreign agent (**Yes**), or only answer them, acting as a home agent (**No**).
- Tunnels are normally initiated **On Demand**; however, you can disable this feature. When disabled, the tunnel must be manually established through the call management screens.
- You can specify the **Idle Timeout**, an inactivity timer, whose expiration will terminate the tunnel. A value of zero disables the timer. Because tunnels are subject to abrupt termination when the underlying datalink is torn down, use of the Idle Timeout is strongly encouraged.
- Return to the Connection Profile screen by pressing Escape.
- Select **IP Profile Parameters** and press Return. The IP Profile Parameters screen appears.

IP Profile Parameters

Address Translation Enabled:	Yes
NAT Map List...	Easy-PAT
NAT Server List...	Easy-Servers
Local WAN IP Address:	0.0.0.0
Remote IP Address:	173.167.8.10
Remote IP Mask:	255.255.0.0
Filter Set...	
Remove Filter Set	
RIP Profile Options...	

- Enter the **Remote IP Address** and **Remote IP Mask** for the host to which you want to tunnel.

Encryption Support

Encryption is a method for altering user data into a form that is unusable by anyone other than the intended recipient. The recipient must have the means to decrypt the data to render it usable to them. The encryption process protects the data by making it difficult for any third party to get at the original data.

Netopia PPTP is fully compatible with Microsoft Point-to-Point Encryption (MPPE) data encryption for user data transfer over the PPTP tunnel. Microsoft Windows NT Server provides MPPE encryption capability only when Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) is enabled. Netopia complies with this feature to allow MPPE only when MS-CHAP is negotiated. MS-CHAP and MPPE are user-selectable options in the PPTP Tunnel Options screen. If either the client or the server side specifies encryption, then encryption becomes mandatory for both.

Netopia's ATMP implementation supports Data Encryption Standard (DES) data encryption for user data transfer over the ATMP tunnel between two Netopia Routers. The encryption option, none or DES, is a selectable option in the ATMP Tunnel Options screen.

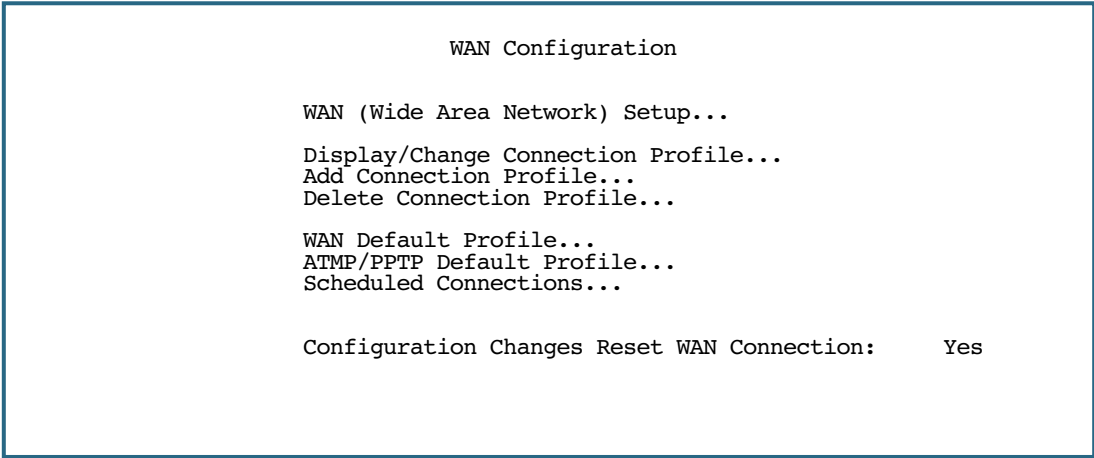
MS-CHAP V2 and 128-bit strong encryption

Notes:

- Netopia Firmware Version 8.4 supports 128-bit (“strong”) encryption when using PPTP tunnels.
ATMP does not have an option of using 128-bit MPPE. If you are using ATMP between two Netopia Routers you can optionally set 56-bit DES encryption.
- When you choose MS-CHAP as the authentication method for a PPTP tunnel, the Netopia Router will start negotiating MS-CHAPv2. If the gateway or VPN adapter client you are connecting to does not support MS-CHAPv2, the Netopia Router will fall back to MS-CHAPv1, or, if the gateway or VPN adapter client you are connecting to does not support MPPE at all, the PPP session will be dropped. This is done automatically and transparently.

ATMP/PPTP Default Profile

The WAN Configuration menu offers a ATMP/PPTP Default Profile option. Use this selection when your Router is acting as the server for VPN connections, that is, when you are on the answering end of the tunnel establishment. The ATMP/PPTP Default Profile determines the way the attempted tunnel connection is answered.



To set the parameters under which the Router will answer attempted VPN connections, select **ATMP/PPTP Default Profile** and press Return. The ATMP/PPTP Default Profile screen appears.

ATMP/PPTP Default Profile

Answer ATMP/PPTP Connections:	No
PPTP Configuration Options	
Receive Authentication...	PAP
Data Compression...	None

- Toggle **Answer ATMP/PPTP Connections** to **Yes** if you want the Router to accept VPN connections or **No** (the default) if you do not.
- For PPTP tunnel connections only, you must define what type of authentication these connections will use. Select **Receive Authentication** and press Return. A pop-up menu offers the following options: PAP (the default), CHAP, or MS-CHAP.
- If you chose PAP or CHAP authentication, from the **Data Compression** pop-up menu select either None (the default) or Standard LZS.

If you chose MS-CHAP authentication, the **Data Compression** option is not required, and this menu item becomes hidden.

VPN QuickView

You can view the status of your VPN connections in the VPN QuickView screen.

From the Main Menu select QuickView and then VPN QuickView.



The VPN QuickView screen appears.

VPN Quick View							
Profile Name-----	Type-----	Rx Pckts---	Tx Pckts--	RxDiscard--	Remote Address--		
HA <-> FA1 (Jony Fon	ATMP	99	99	0	173.166.82.8		
HA <-> FA3 (Sleve M.	ATMP	13	14	0	173.166.117.91		

- Profile Name:** Lists the name of the Connection Profile being used, if any.
- Type:** Shows the data link encapsulation method (PPTP or ATMP).
- Rx Pckts:** Shows the number of packets received via the VPN tunnel.
- Tx Pckts:** Shows the number of packets transmitted via the VPN tunnel.
- Rx Discard:** Shows the number of packets discarded.
- Remote Address:** Shows the tunnel partner’s IP address.

Dial-Up Networking for VPN

Microsoft Windows Dial-Up Networking software permits a remote standalone workstation to establish a VPN tunnel to a PPTP server such as a Netopia Router located at a central site. Dial-Up Networking also allows a mobile user who may not be connected to a PAC to dial into an intermediate ISP and establish a VPN tunnel to, for example, a corporate headquarters, remotely. Netopia Routers also can serve as a PAC at the workstation's site, making it unnecessary for the standalone workstation to initiate the tunnel. In such a case, the Dial-Up Networking software is not required, since the Netopia Router initiates the tunnel.

This section is provided for users who may require the VPN client software for Dial-Up Networking in order to connect to an ISP who provides a PPTP account.

Microsoft Windows Dial-Up Networking (DUN) is the means by which you can initiate a VPN tunnel between your individual remote client workstation and a private network such as your corporate LAN via the Internet. DUN is a software adapter that allows you to establish a tunnel.

DUN is a free add-on available for Windows 95, and comes standard with Windows 98 and Windows NT. The VPN tunnel behaves as a private network connection, unrelated to other traffic on the network. Once you have installed Dial-Up Networking, you will be able to connect to your remote site as if you had a direct private connection, regardless of the intervening network(s) through which your data passes. You may need to install the Dial-Up Networking feature of Windows 95, 98, or 2000 to take advantage of the virtual private networking feature of your Netopia Router.

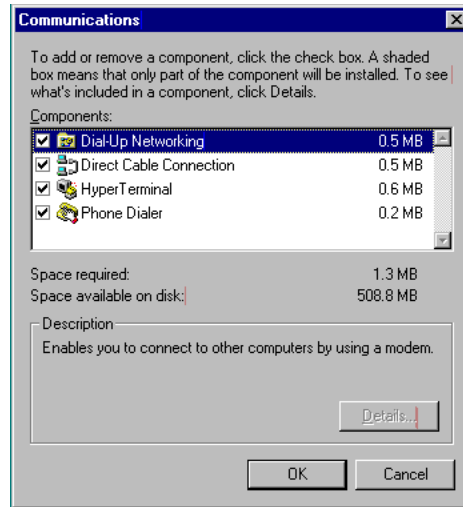
Note: For the latest information and tech notes on Dial-Up Networking and VPNs be sure to visit the Netopia website at <http://www.netopia.com> and, for the latest software and release notes, the Microsoft website at <http://www.microsoft.com>.

Installing Dial-Up Networking

Check to see if Dial-Up Networking is already installed on your PC. Open your My Computer (or whatever you have named it) icon on your desktop. If there is a folder named Dial-Up Networking, you don't have to install it. If there is no such folder, you must install it from your system disks or CDROM. Do the following:

1. From the **Start** menu, select **Settings** and then **Control Panel**.
2. In the Control Panel window, double-click the **Add/Remove Programs** icon.
The Add/Remove Programs Properties window appears.
3. Click the **Windows Setup** tab.
4. Double-click **Communications**.

The Communications window appears.



5. In the Communications window, select **Dial-Up Networking** and click the **OK** button.
This returns you to the Windows Setup screen. Click the **OK** button.
6. Respond to the prompts to install Dial-Up Networking from the system disks or CDROM.
7. When prompted, reboot your PC.

Creating a new Dial-Up Networking profile

A Dial-Up Networking profile is like an address book entry that contains the information and parameters you need for a secure private connection. You can create this profile by using either the Internet Connection Wizard or the Make New Connection feature of Dial-Up Networking. The following instructions tell you how to create the profile with the Make New Connection feature. Do the following:

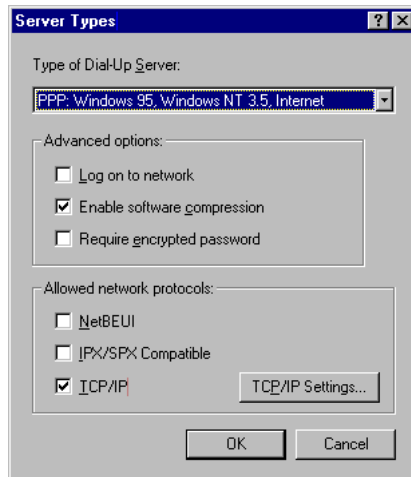
1. Double-click the **My Computer** (or whatever you have named it) icon on your desktop.
Open the Dial-Up Networking folder, and then double-click **Make New Connection**. The Make New Connection wizard window appears.
2. Type a name for this connection (such as the name of your company, or the computer you are dialing into).
From the pull-down menu, select the device you intend to use for the virtual private network connection. This can be any device you have installed or connected to your PC. Click the **Next** button. A screen appears with fields for you to enter telephone numbers for the computer you want to connect to.
3. Type the directory number or the **Virtual Circuit Identifier** number.
This number is provided by your ISP or corporate administrator. Depending on the type of device you are using, the number may or may not resemble an ordinary telephone directory number.
4. Click the **Next** button.
The final window will give you a chance to accept or change the name you have entered for this profile. If you are satisfied with it, click the **Finish** button. Your profile is complete.

Configuring a Dial-Up Networking profile

Once you have created your Dial-Up Networking profile, you configure it for TCP/IP networking to allow you to connect to the Internet through your Internet connection device. Do the following:

1. Double-click the **My Computer** (or whatever you have named it) icon on your desktop.
Open the Dial-Up Networking folder. You will see the icon for the profile you created in the previous section.
2. Right-click the icon and from the pop-up menu select **Properties**.
3. In the Properties window click the **Server Type** button.

From the Type of Dial-up Server pull-down menu select the appropriate type of server for your system version:



- Windows 95 users select **PPP: Windows 95, Windows NT 3.5, Internet**
- Windows 98 users select **PPP: Windows 98, Windows NT Server, Internet**

In the Allowed network protocols area check **TCP/IP** and uncheck all of the other checkboxes.

Note: Netopia's PPTP implementation does not currently support tunnelling of IPX and NetBEUI protocols.

- Click the **TCP/IP Settings** button.

- If your ISP uses dynamic IP addressing (DHCP), select the Server assigned IP address radio button.
 - If your ISP uses static IP addressing, select the Specify an IP address radio button and enter your assigned IP address in the fields provided. Also enter the IP address in the Primary and Secondary DNS fields.
- Click the **OK** button in this window and the next two windows.

Connecting using Dial-Up Networking

A Dial-Up Networking connection will be automatically launched whenever you run a TCP/IP application, such as a web browser or email client. When you first run the application a Connect To dialog box appears in which you enter your User name and Password. If you check the Save password checkbox, the system will remember your User name and Password, and you won't be prompted for them again.

Allowing VPNs through a Firewall

An administrator interested in securing a network will usually combine the use of VPNs with the use of a firewall or some similar mechanism. This is because a VPN is not a complete security solution, but rather a component of overall security. Using a VPN will add security to transactions carried over a public network, but a VPN alone will not prevent a public network from infiltrating a private network. Therefore, you should combine use of a firewall with VPNs, where the firewall will secure the private network from infiltration from a public network, and the VPN will secure the transactions that must cross the public network.

A strict firewall may not be provisioned to allow VPN traffic to pass back and forth as needed. In order to ensure that a firewall will allow a VPN, certain attributes must be added to the firewall's provisioning. The provisions necessary vary slightly between ATMP and PPTP, but both protocols operate on the same basic premise: there are control and negotiation operations, and there is the tunnelled traffic that carries the payload of data between the VPN endpoints. The difference is that ATMP uses UDP to handle control and negotiation, while PPTP uses TCP. Then both ATMP and PPTP use GRE to carry the payload.

For PPTP negotiation to work, TCP packets inbound and outbound destined for port 1723 must be allowed. Likewise, for ATMP negotiation to work, UDP packets inbound and outbound destined for port 5150 must be allowed. Source ports are dynamic, so, if possible, make this flexible, too. Additionally, PPTP and ATMP both require a firewall to allow GRE bi-directionally.

The following sections illustrate a sample filtering setup to allow either PPTP or ATMP traffic to cross a firewall:

- ["PPTP example" on page 4-26](#)
- ["ATMP example" on page 4-28](#)

Make your own appropriate substitutions. For more information on filters and firewalls, see [Chapter 9, "Security."](#)

PPTP example

To enable a firewall to allow PPTP traffic, you must provision the firewall to allow inbound and outbound TCP packets specifically destined for port 1723. The source port may be dynamic, so often it is not useful to apply a compare function upon this portion of the control/negotiation packets. You must also set the firewall to allow inbound and outbound GRE packets, enabling transport of the tunnel payload.

From the Main Menu navigate to Display/Change IP Filter Set, and from the pop-up menu select **Basic Firewall**.



Select **Display/Change Input Filter**.

Display/Change Input Filter screen

+---#----	Source IP Addr----	Dest IP Addr-----	Proto-	Src.Port-	D.Port--	On?--	Fwd--	+
1	0.0.0.0	0.0.0.0	TCP	NC	=2000	Yes	No	
2	0.0.0.0	0.0.0.0	TCP	NC	=6000	Yes	No	

Select Input Filter 1 and press Return. In the Change Input Filter 1 screen, set the Destination Port information as shown below.

Change Input Filter 1

Enabled:

Forward:

Yes

Yes

Source IP Address:

Source IP Address Mask:

0.0.0.0

0.0.0.0

Dest. IP Address:

Dest. IP Address Mask:

0.0.0.0

0.0.0.0

Protocol Type:

Source Port Compare...

Source Port ID:

Dest. Port Compare...

Dest. Port ID:

Established TCP Conns. Only:

TCP

No Compare

0

Equal

1723

No

Select Input Filter 2 and press Return. In the Change Input Filter 2 screen, set the Protocol Type to allow GRE as shown below.

Change Input Filter 2

Enabled:

Yes

Forward:

Yes

Source IP Address:

0.0.0.0

Source IP Address Mask:

0.0.0.0

Dest. IP Address:

0.0.0.0

Dest. IP Address Mask:

0.0.0.0

Protocol Type:

GRE

In the Display/Change Filter Set screen select **Display/Change Output Filter**.

Display/Change Output Filter screen

+ #	Source IP Addr	Dest IP Addr	Proto	Src.Port	D.Port	On?	Fwd?
1	0.0.0.0	0.0.0.0	TCP	NC	=1723	Yes	Yes
2	0.0.0.0	0.0.0.0	GRE	--	--	Yes	Yes

Select Output Filter 1 and press Return. In the Change Output Filter 1 screen, set the Protocol Type and Destination Port information as shown below.

Change Output Filter 1

Enabled:

Yes

Forward:

Yes

Source IP Address:

0.0.0.0

Source IP Address Mask:

0.0.0.0

Dest. IP Address:

0.0.0.0

Dest. IP Address Mask:

0.0.0.0

Protocol Type:

TCP

Source Port Compare...

No Compare

Source Port ID:

0

Dest. Port Compare...

Equal

Dest. Port ID:

1723

Established TCP Conns. Only:

No

Select Output Filter 2 and press Return. In the Change Output Filter 2 screen, set the Protocol Type to allow GRE as shown below.

Change Output Filter 2

Enabled:

Forward:

Source IP Address:

Source IP Address Mask:

Dest. IP Address:

Dest. IP Address Mask:

Protocol Type:

Yes

Yes

0.0.0.0

0.0.0.0

0.0.0.0

0.0.0.0

GRE

ATMP example

To enable a firewall to allow ATMP traffic, you must provision the firewall to allow inbound and outbound UDP packets specifically destined for port 5150. The source port may be dynamic, so often it is not useful to apply a compare function on this portion of the control/negotiation packets. You must also set the firewall to allow inbound and outbound GRE packets (Protocol 47, Internet Assigned Numbers Document, RFC 1700), enabling transport of the tunnel payload.

From the Main Menu navigate to Display/Change IP Filter Set, and from the pop-up menu select **Basic Firewall**.



Select **Display/Change Input Filter**.

Display/Change Input Filter screen

+	--#----	Source IP Addr----	Dest IP Addr-----	Proto-	Src.Port-	D.Port--	On?	Fwd--	+
1		0.0.0.0	0.0.0.0	TCP	NC	=2000	Yes	No	
2		0.0.0.0	0.0.0.0	TCP	NC	=6000	Yes	No	

Select Input Filter 1 and press Return. In the Change Input Filter 1 screen, set the Destination Port information as shown below.

Change Input Filter 1	
Enabled:	Yes
Forward:	Yes
Source IP Address:	0.0.0.0
Source IP Address Mask:	0.0.0.0
Dest. IP Address:	0.0.0.0
Dest. IP Address Mask:	0.0.0.0
Protocol Type:	TCP
Source Port Compare...	No Compare
Source Port ID:	0
Dest. Port Compare...	Equal
Dest. Port ID:	1723
Established TCP Conns. Only:	No

Select Input Filter 2 and press Return. In the Change Input Filter 2 screen, set the Protocol Type to allow GRE as shown below.

Change Input Filter 2	
Enabled:	Yes
Forward:	Yes
Source IP Address:	0.0.0.0
Source IP Address Mask:	0.0.0.0
Dest. IP Address:	0.0.0.0
Dest. IP Address Mask:	0.0.0.0
Protocol Type:	GRE

In the Display/Change Filter Set screen select **Display/Change Output Filter**.

Display/Change Output Filter screen

+ #	Source IP Addr	Dest IP Addr	Proto	Src.Port	D.Port	On?	Fwd?
1	0.0.0.0	0.0.0.0	TCP	NC	=1723	Yes	Yes
2	0.0.0.0	0.0.0.0	GRE	--	--	Yes	Yes

Select Output Filter 1 and press Return. In the Change Output Filter 1 screen, set the Protocol Type and Destination Port information as shown below.

Change Output Filter 1

Enabled:

Yes

Forward:

Yes

Source IP Address:

0.0.0.0

Source IP Address Mask:

0.0.0.0

Dest. IP Address:

0.0.0.0

Dest. IP Address Mask:

0.0.0.0

Protocol Type:

UDP

Source Port Compare...

No Compare

Source Port ID:

0

Dest. Port Compare...

No Compare

Dest. Port ID:

5150

Select Output Filter 2 and press Return. In the Change Output Filter 2 screen, set the Protocol Type to allow GRE as shown below.

Change Output Filter 2

Enabled:

Yes

Forward:

Yes

Source IP Address:

0.0.0.0

Source IP Address Mask:

0.0.0.0

Dest. IP Address:

0.0.0.0

Dest. IP Address Mask:

0.0.0.0

Protocol Type:

GRE

Windows Networking Broadcasts

Netopia firmware provides the ability to forward Windows Networking NetBIOS broadcasts. This is useful for, for example, a Virtual Private Network, in which you want to be able to browse the remote network to which you are tunnelling, as part of your Windows Network Neighborhood.

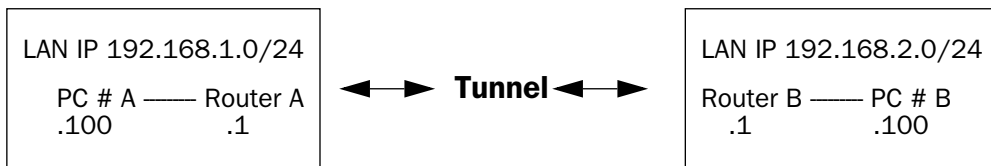
Routed connections, such as VPNs, can not use NetBEUI to carry the Network Neighborhood information. They need to use NetBIOS, because NetBEUI cannot be routed. This feature will allow browsing the Network Neighborhood without any additional workstation configuration.

You enable this feature in the **IP Profile Parameters** screen of your Connection Profile. The IP Profile Parameters screen varies slightly, depending on whether your model router connects directly to the Internet, or if it connects via an Ethernet connection through a cable or DSL modem. The enabling feature is the same for both:

Using the Tab key, toggle **NetBIOS Proxy Enabled** from the default **No** to **Yes**, and press Return. Your remote Network Neighborhood becomes accessible from your Windows desktop.

Note: The remote IP address and subnet mask should strictly match the IP address and subnet mask configured on the LAN interface of the remote router. See the following example.

Example:



When PC #A sends a Windows networking broadcast it sends it with a destination IP 192.168.1.255.

When Router A receives this broadcast it translates the destination of this broadcast to match the remote IP of the NetBIOS Proxy-enabled VPN profiles and it forwards the broadcast through the VPN tunnel.

When Router B receives this broadcast, it sends it on its LAN.

Configuration for Router A

IP Profile Parameters

Address Translation Enabled:

No

Remote IP Address:

192.168.2.1

Remote IP Mask:

255.255.255.0

Filter Set...

Remove Filter Set

NetBIOS Proxy Enabled

Yes

RIP Profile Options...

Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
Configure IP requirements for a remote network connection here.

Configuration for Router B

IP Profile Parameters

Address Translation Enabled:

No

Remote IP Address:

192.168.1.1

Remote IP Mask:

255.255.255.0

Filter Set...

Remove Filter Set

NetBIOS Proxy Enabled

Yes

RIP Profile Options...

Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
Configure IP requirements for a remote network connection here.

Note: Microsoft Network browsing is available with or without a Windows Internet Name Service (WINS) server. Shared volumes on the remote network are accessible with or without a WINS server. Local LAN shared volumes that have Port Address Translation (PAT) applied to them are *not* available to hosts on the remote LAN. For tunnelled traffic, NAT on the WAN has no effect on the Microsoft Networking traffic.

Make sure the NetBIOS filter is not enabled in your Internet Connection Profile.

Netopia includes the NetBIOS Proxy feature as an enhancement and convenience for our customers. It has been lab-tested and many customers use it successfully. However, Netopia cannot guarantee that this feature will automatically give you the networking functionality you expect. There are many possible issues with the various Windows operating systems that may prevent NetBIOS from functioning as described above. Netopia Technical Support does not troubleshoot problems customers may encounter with their Windows operating system

Chapter 5

Internet Key Exchange (IKE) IPsec Key Management for VPNs

IPsec stands for IP Security, a set of protocols that supports secure exchange of IP packets at the IP layer. IPsec is deployed widely to implement Virtual Private Networks (VPNs). See [“Virtual Private Networks \(VPNs\)” on page 4-1](#) for more information.

The Netopia Firmware Version 8.4 supports Internet Key Exchange (IKE) for secure encrypted communication over a VPN tunnel.

This chapter covers the following topics:

- [“Overview” on page 5-1](#)
- [“Internet Key Exchange \(IKE\) Configuration” on page 5-2](#)
- [“Key Management” on page 5-8](#)
- [“IPsec WAN Configuration Screens” on page 5-18](#)
- [“IPsec Manual Key Entry” on page 5-19](#)

Overview

IPsec supports two encapsulation modes: Transport and Tunnel. Transport mode encrypts only the data portion (payload) of each packet, but leaves the header untouched. Tunnel mode encrypts both the header and the payload. On the receiving side, an IPsec-compliant device decrypts each packet. Netopia Routers support Tunnel mode.

DES stands for Data Encryption Standard, a popular symmetric-key encryption method. DES uses a 56-bit key. Netopia Routers offer IPsec 3DES (triple DES) encryption as a standard option.

Internet Key Exchange (IKE) is an authentication and encryption key management protocol used in conjunction with the IPsec standard.

IKE is a two-phase protocol for key exchange.

- Phase 1 authenticates the security gateways and establishes the *Security Parameters* (SPs) they will use to negotiate on behalf of the clients. *Security Associations* (SAs) are sets of information values that allow the two devices on the Internet to communicate securely.
- Phase 2 establishes the tunnel and provides for secure transport of data.

IPsec can be configured without IKE, but IKE offers additional features, flexibility, and ease of configuration. Key exchange between your local Router and a remote point can be configured either manually or by using the key exchange protocol.

The advantage of using IKE is that it automatically negotiates IPsec Security Associations and enables IPsec secure communications without having to manually enter the lengthy encryption keys at both ends of the connection. You enter a human-readable pass phrase or shared secret English sentence, like “my dog has fleas” on each end once. This pass phrase is used to authenticate each end to the other. Thereafter, the two ends periodically use a public key encryption method called Diffie-Hellman to exchange key material and then securely generate new authentication and encryption keys. The keys are automatically and continually changing, making the data exchanged using the keys inherently secure.

It also allows you to specify a lifetime for the IPsec Security Association and allows encryption keys to change periodically during IPsec sessions. You can set this period for key generation to as often as your security requirements dictate.

A *Security Policy Database (SPD)* now defines the security requirements. This is a significant change from earlier firmware implementations of IPsec. Traffic with a source IP address that falls within the local member specification of an IPsec tunnel and that is addressed to a destination IP address that falls within the remote member specification of that tunnel is not routed using the normal routing table. Instead it is forwarded using the security policy database to the remote security gateway (remote tunnel endpoint) specified in the IPsec tunnel configuration. It is not possible to send traffic outside the tunnel by bypassing the tunnel and the remote security gateway.

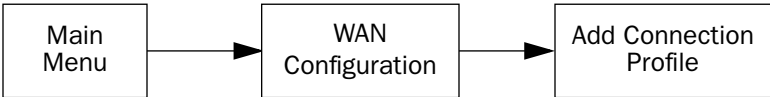
Note: To fully protect against IP address “spoofing” of local member addresses requires firewall rules to be installed on the WAN interface. These must prevent packets coming in through that interface with local member source addresses, since local member source addresses should only originate from the LAN. Otherwise it is theoretically possible for a malicious hacker to send packets through the tunnel by impersonating local member IP addresses. See the chapter [“Security” on page 9-1](#) for more information.

Traffic originating from local member LAN addresses that is not addressed to remote member addresses, as well as traffic originating from local LAN IP addresses that do not match any local member specifications, is routed using the normal routing table. This means that if you want to restrict traffic from local members from going out to the Internet and force it all to go through one or more tunnels you need to specify remote members of 0.0.0.0 - 255.255.255.255 or 0.0.0.0/0. Traffic originating from the gateway, for example, Telnet, ping, DNS queries, will not use the default VPN definition even if the source addresses match. Traffic to and from the gateway is included in specific VPNs.

Internet Key Exchange (IKE) Configuration

IPsec tunnels are defined in the same manner as PPTP tunnels. (See [“Virtual Private Networks \(VPNs\)” on page 4-1](#) for more information.) You configure the Connection Profile as follows.

From the Main Menu navigate to WAN Configuration and then Add Connection Profile.



The Add Connection Profile screen appears.

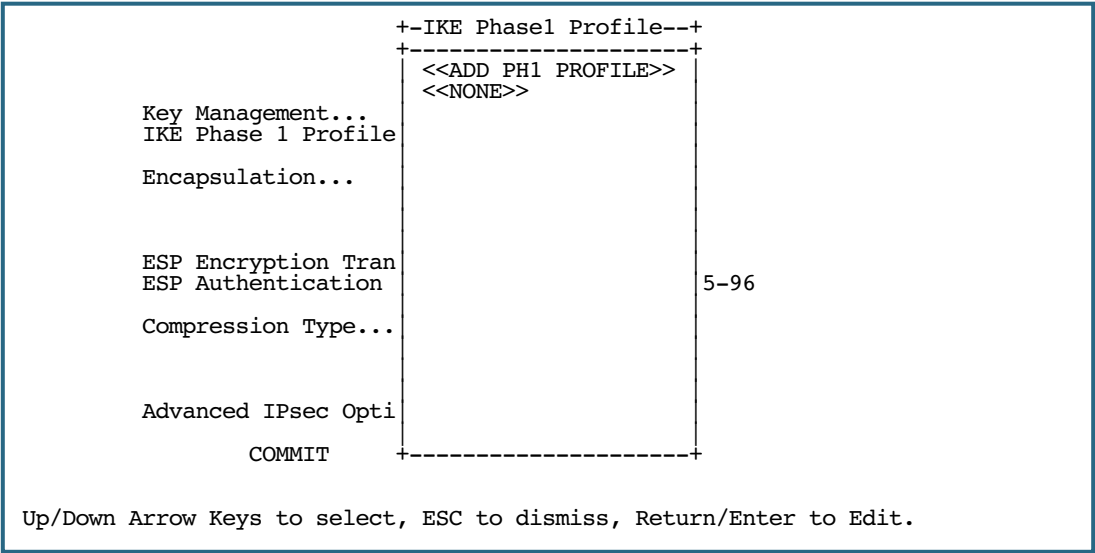
Add Connection Profile	
Profile Name:	Profile 1
Profile Enabled:	<input checked="" type="checkbox"/>
Encapsulation Type...	<div> <div>PPP</div> <div>RFC1483</div> <div>ATMP</div> <div>PPTP</div> <div>IPsec</div> <div>L2TP</div> </div>
RFC1483 Mode...	
IP Profile Parameters...	
<div> <div>COMMIT</div> <div>CANCEL</div> </div>	

- From the **Encapsulation Type** pop-up menu select **IPsec**.
- Then select **Encapsulation Options**. The IPsec Tunnel Options screen appears.

IPsec Tunnel Options	
Key Management...	IKE
IKE Phase 1 Profile...	
Encapsulation...	ESP
ESP Encryption Transform...	DES
ESP Authentication Transform...	HMAC-MD5-96
Compression Type...	None
Advanced IPsec Options...	
<div> <div>COMMIT</div> <div>CANCEL</div> </div>	

For **Key Management** you can use either **IKE** or **Manual**. If you choose Manual, skip to [“IPsec Manual Key Entry” on page 5-19](#). If you choose IKE (the default) continue below.

- Select **IKE Phase 1 Profile** and press Return.

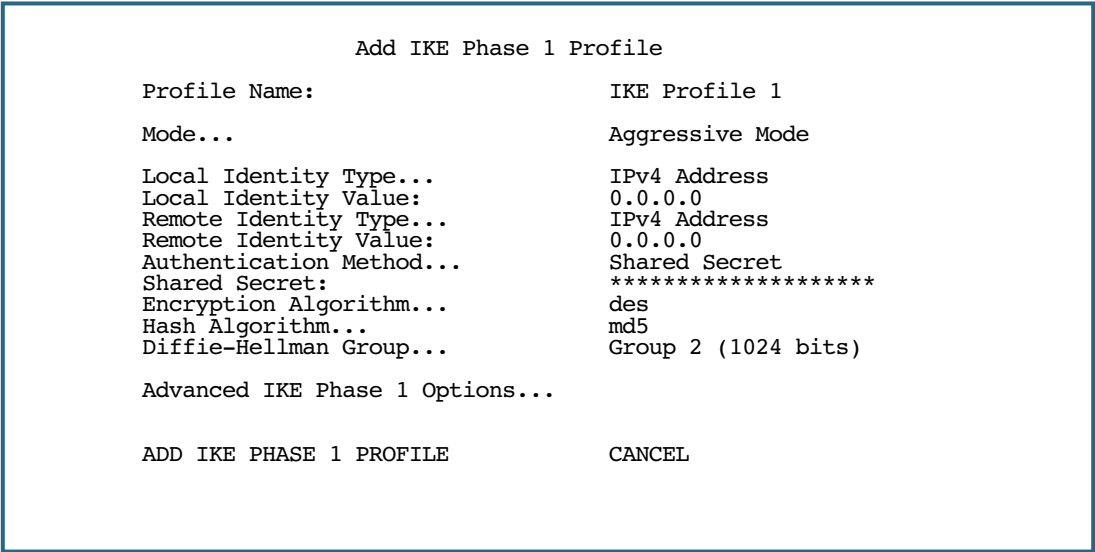


- A pop-up window displays a list of IKE Phase 1 Profiles that you have configured. If you have not previously configured an IKE Phase 1 Profile, the selection **ADD PH1 PROFILE** allows you to do that now.

Adding an IKE Phase 1 Profile

IKE Phase 1 Profiles contain the information that the two ends of a tunnel use to authenticate each other and the parameters that govern the public key cryptography exchanges that are required to generate new keys periodically. Make sure to add an IKE Phase 1 Profile. If an IKE Phase 1 Profile is not assigned to an IKE Connection Profile, all VPN traffic for that profile will be discarded.

Select **ADD PH1 PROFILE**. The Add IKE Phase 1 Profile screen appears.



- The **Profile Name** field accepts any name of up to 16 characters. Sixteen IKE Phase 1 profiles are supported, since each of the potential sixteen Connection Profiles may be associated with a separate IKE Phase 1 profile.
- The **Mode** pop-up menu allows you to choose between Main Mode (the default) and Aggressive Mode.
- In **Main Mode** the Router hides the **Local** and **Remote Identity Type** and **Value** fields, defaults to the host address, and always uses the IPV4 Address and the local and remote tunnel endpoint address.
- In **Aggressive Mode** the **Local** and **Remote Identity Type** pop-up menus allow you to choose the type of Identity value to use: IPV4 Address, IPV4 Subnet, IPV4 Range, Host Name, E-Mail Address, Key ID (ASCII), and Key ID (HEX). The **Local** and **Remote Identity Type** and **Value** menus allow you to specify one of the following, based on what Local Identity Type you selected in the previous pop-up menu:

IPV4 Address: A single IPV4 address in the familiar dotted-quad notation (a.b.c.d).

IPV4 Subnet: A single IPV4 network address in dotted-quad notation (a.b.c.d) followed by a mask specified *either* by a slash and a bit-count between 0 and 32 OR by a second dotted-quad.

IPV4 Range: Two IPV4 addresses in dotted quad notation (a.b.c.d) separated by a space.

Host Name: A fully-qualified domain name (FQDN).

E-Mail Address: An RFC 822 e-mail address in the form *user@hostname*.

Key ID (ASCII): An opaque string consisting of printable ASCII characters represented as a sequence of printable ASCII characters.

Key ID (HEX): An opaque string consisting of arbitrary 8-bit ASCII values represented as a sequence of hexadecimal digits, each of which corresponds to one nibble of the string value.

- The **Authentication Method** pop-up menu specifies the IKE Phase 1 authentication method. The only currently supported authentication method is Shared Secret. Other methods may be supported in future firmware releases.
- The **Shared Secret** field allows you to enter a shared secret phrase (between 1 and 48 characters long) that will be used to generate key material for IKE Phase 1.
- The **Encryption Algorithm** pop-up menu specifies the IKE Phase 1 encryption algorithm, and may be either DES (the default) or 3DES.
- The **Hash Algorithm** pop-up menu specifies the IKE Phase 1 hash algorithm, and may be either SHA1 (the default) or MD5.
- The **Diffie-Hellman Group** pop-up menu specifies the IKE Phase 1 Diffie-Hellman key exchange size, and may be either Group 1 (768 bits), Group 2 (1024 bits) (the default), or Group 5 (1536 bits).
- If you select **Advanced IKE Phase 1 Options** the Advanced IKE Phase 1 Options screen appears.

Advanced IKE Phase 1 Options	
Negotiation...	Normal
SA Use Policy...	Newest SAs Immediately
Allow Dangling Phase 2 SAs:	Yes
Phase 1 SA Lifetime (seconds):	28800
Send Initial Contact Message:	Yes
Include Vendor ID Payload:	Yes
Independent Phase 2 Re-keys:	Yes
Strict Port Policy:	No

Return/Enter accepts * Tab toggles * ESC cancels.

Normally it is not necessary to change the settings of the items on the Advanced IKE Phase 1 Options screen. Most of these settings exist for ensuring compatibility with remote IKE implementations that may have certain limitations.

- The **Negotiation** pop-up menu allows you to specify the way the device will respond to a connection attempt. Normal (the default) is a two-way mode; Initiate Only or Respond Only permit limiting the connection to one-way only.
- The **SA Use Policy** pop-up menu specifies the policy that the Router will use to determine which Phase 1 SAs to use when multiple valid Phase 1 SAs are available for transmitting traffic on an IPsec tunnel.
Because the Router normally re-keys prior to the expiration of the current Phase 1 SAs, multiple valid Phase 1 SAs may exist during the period of time after the Router has re-keyed and established new Phase 1 SAs and the time at which the old Phase 1 SAs expire.
 - If you select **Newest SAs Immediately**, the Router will begin using the newly created Phase 1 SAs immediately after they are negotiated.
 - If you select **Old SAs Until Expired**, the Router will continue using the old Phase 1 SAs until they expire and will begin using the newly created Phase 1 SAs only after the old ones are no longer valid.
- **Allow Dangling Phase 2 SAs** toggles whether or not Phase 2 SAs are permitted to survive the expiration of the Phase 1 SAs under which they were created. Phase 2 SAs “dangle” when the Phase 1 SA under which they were created expires before they do. There is no requirement that the Phase 1 SA exist for the duration of the Phase 2 SA’s lifetime, but it is convenient because a Delete message may be sent.
- **Phase 1 SA Lifetime (seconds)** specifies the duration in seconds for which the SA will remain valid. The range of permissible values is the set of non-negative integer values between 0 and $2^{32}-1$. The default value is 28,800 seconds. The value zero specifies the default.
- **Send Initial Contact Message** toggles whether or not the IKE negotiation process begins by sending an initial contact message. The default is **Yes**.

- **Include Vendor-ID Payload** toggles whether or not the Router includes the vendor-ID payload in its IKE Phase 1 messages.
- **Independent Phase 2 Re-keys** toggles whether or not a Phase 2 re-keys requires a Phase 1 re-key. If this item is set to Yes (the default), Phase 2 re-keys will be performed independently when necessary without requiring a Phase 1 re-key. If this item is set to No, each Phase 2 re-key will be preceded by a Phase 1 re-key. This item should normally be set to Yes unless the device is communicating with a non-compliant remote IPsec peer that requires that a Phase 1 re-key precede each Phase 2 re-key.
- **Strict Port Policy** toggles whether or not IKE requires packets to originate from the IANA IKE port (500). Set to **Yes**, the Router will listen only to port 500 and source its packets from port 500. Set to **No**, the Router will return traffic to whatever port originated it.

Changing an IKE Phase 1 Profile

Selecting **Display/Change IKE Phase 1 Profile** or **Delete IKE Phase 1 Profile** displays an IKE Phase 1 profile pop-up menu listing the names of all currently defined IKE Phase 1 profiles:

```

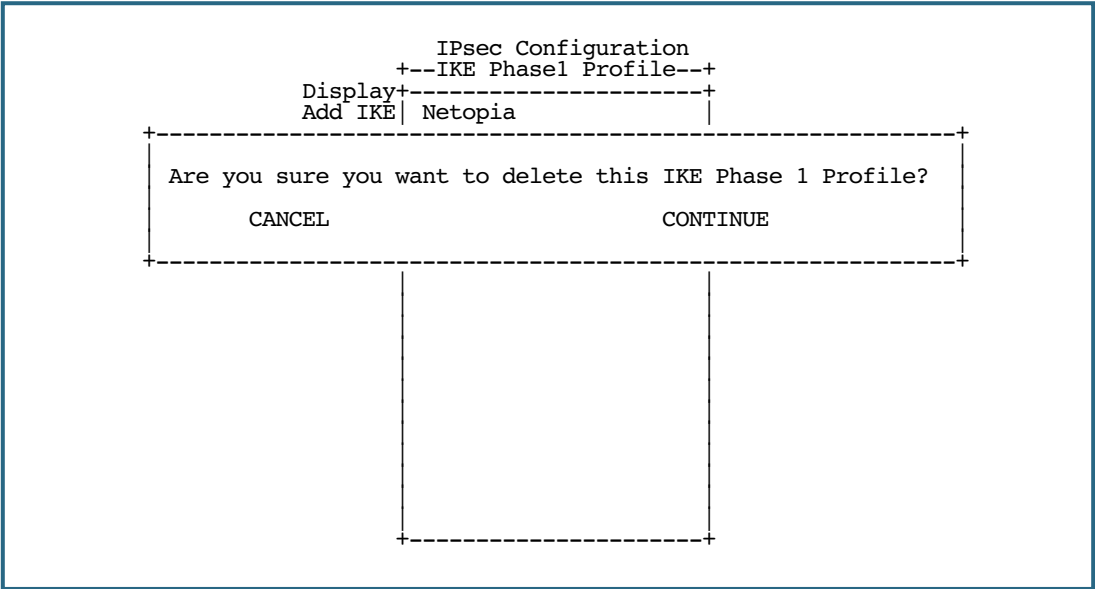
                                IPsec Configuration
                                +--IKE Phase1 Profile--+
                                +-----+
D  IKE Profile 2                | 1 Profile...
A  Arthropods                  | .
D  Anthropoids                  | e...
    Anopheles
    Albigensians
                                +-----+

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

```

Selecting **Display/Change IKE Phase 1 Profile** and choosing an IKE phase 1 profile name from the pop-up list displays the Change IKE Phase 1 Profile screen. This screen is identical to the Add IKE Phase 1 Profile screen shown above.

Selecting **Delete IKE Phase 1 Profile** and choosing an IKE phase 1 profile name from the pop-up list displays a confirmation alert asking you to confirm that you really want to delete the specified IKE phase 1 profile:



Key Management

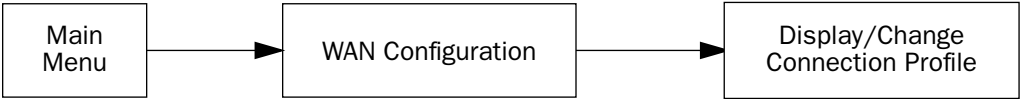
You specify your IKE key management on a per-Connection Profile basis. You can do this in one of three ways:

- You can create your IKE Phase 1 Profile first, and then associate it with an existing Connection Profile
- You can create a Connection Profile and then modify it to associate it with an existing IKE Phase 1 Profile
- You can create a new Connection Profile and add a new IKE Phase 1 Profile as you go

You can do this WAN Configuration menus.

Refer to [“Creating a New Connection Profile” on page 2-9](#) for instructions on creating a Connection Profile if you don’t already know how to do that.

You can access the Key Management menus from the Change Connection Profile menu under the WAN Configuration screen for a Connection Profile you have already created,



or you can create a new Connection Profile with your IKE settings included, as you go.

The IKE Key management settings are part of the Data Link Options that you specify in the Add Connection Profile or Change Connection Profile menus. In this description, it is assumed that you are changing an existing Connection Profile.

A Change Connection Profile screen is shown below.

Change Connection Profile

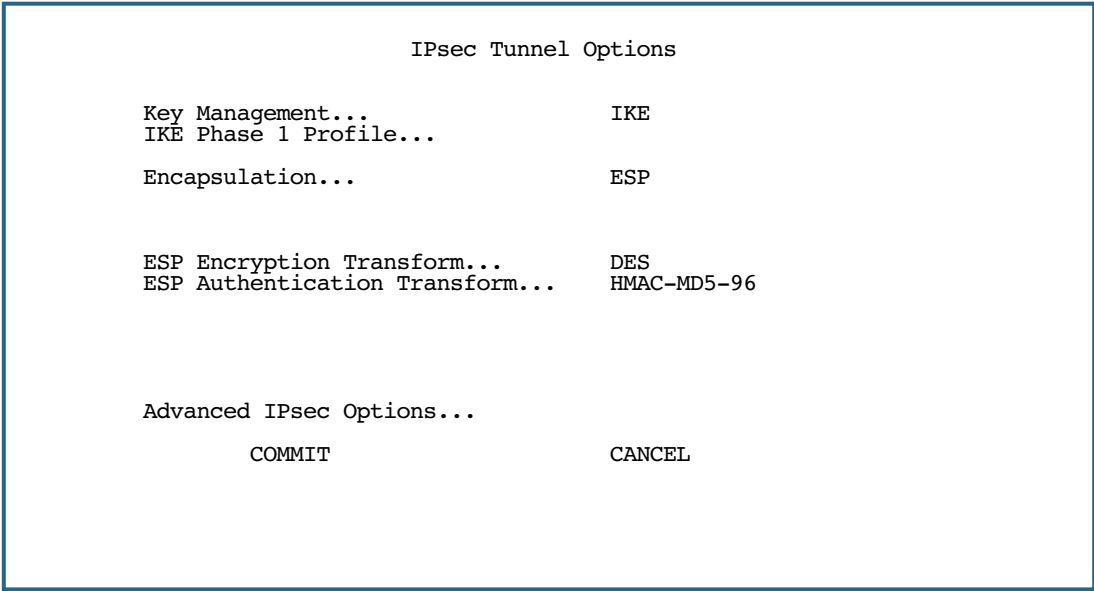
Profile Name:	Easy Setup Profile
Profile Enabled:	+
Encapsulation Type...	+
Encapsulation Options...	<div style="border: 1px solid black; padding: 5px; text-align: left;"> PPP ATMP PPTP IPsec </div>
IP Profile Parameters...	+
Telco Options...	
COMMIT	CANCEL

Note: The Change Connection Profile screen will offer different options, depending on the model of gateway you are using. You can associate an IPsec profile with the Primary, the Backup, or choose to apply it to Any Port of the WAN interface by choosing the interface from the Interface Group pop-up menu as shown below.

Add Connection Profile

Profile Name:	Profile 1
Profile Enabled:	Yes
Encapsulation Type...	IPsec
Encapsulation Options...	
IP Profile Parameters...	
Interface Group...	<div style="border: 1px solid black; padding: 5px; text-align: left;"> Primary Backup Any Port </div>
COMMIT	CANCEL

From the Encapsulation Type pop-up menu, select **IPsec**. Then select **Encapsulation Options** and press Return. The IPsec Tunnel Options screen appears.



The **Key Management** pop-up menu at the top of the IPsec Tunnel Options screen allows you to choose between IKE key management (the default for a new IPsec profile) and Manual key management.

If you select **Manual**, the IKE Phase 1 Profile option does not display, and you must enter your IPsec Manual Keys under the IPsec Manual Keys screen. See “IPsec Manual Key Entry” on page 19.

- The **IKE Phase 1 Profile** pop-up menu allows you to associate an IKE Phase 1 Profile with the IPsec tunnel. An IKE Phase 1 Profile specifies the set of parameters that will be used for the IKE Phase 1 exchange. IKE Phase 1 Profiles may be shared by multiple IPsec tunnels. The pop-up menu item displays the name of the currently associated IKE Phase 1 Profile, if any, or is blank if no IKE Phase 1 profile is associated with the tunnel.

The pop-up menu lists the names of all currently defined IKE Phase 1 Profiles. The pop-up menu also includes an <<ADD PH1 PROFILE>> item to allow you to define a new IKE Phase 1 Profile directly without first going to the IPsec Configuration screen, and a <<NONE>> item to allow you to dissociate an existing IKE Phase 1 Profile from the IPsec tunnel.

The remainder of the screen allows you to configure the IKE Phase 2 parameters that control the contents of the single IKE Phase 2 proposal sent by the Router. These same items specify the values that must be offered by one of the remote peer’s proposals.

- The **Encapsulation** pop-up menu allows you to select what IPsec encapsulations will be used: ESP only (the default), AH only, or AH+ESP (both AH and ESP).
- An **AH Authentication Transform** pop-up menu (which is visible only if you have selected AH or AH+ESP encapsulation) allows you to specify the type of AH authentication: HMAC-MD5-96 or HMAC-SHA1-96.
- The **ESP Encryption Transform** pop-up menu (which is visible only if you have selected ESP or AH+ESP encapsulation) allows you to specify the type of ESP encryption: DES, 3DES, or NULL (no encryption).

- The **ESP Authentication Transform** pop-up menu (which is visible only if you have selected ESP or AH+ESP encapsulation) allows you to specify the type of ESP authentication: None, HMAC-MD5-96, or HMAC-SHA1-96.

Advanced IPsec Options

If you select **Advanced IPsec Options**, the Advanced IPsec Options screen appears.

Advanced IPsec Options	
SA Lifetime seconds:	28800
SA Lifetime Kbytes:	0
Perfect Forward Secrecy:	Yes
Dead Peer Detection:	No
Maximum Packet Size:	1500

This screen allows you to specify the lifetime associated with each IPsec Security Association (SA) and control when the SA will expire and become invalid.

- **SA Lifetime (seconds)** specifies the duration in seconds for which the SA will remain valid. The range of permissible values is the set of non-negative integer values between 0 and $2^{32}-1$. The default value is 28,800 seconds (1 hour). The value zero specifies the absence of an elapsed time lifetime.
- **SA Lifetime (Kilobytes)** specifies the maximum number of kilobytes of data that may be secured (encrypted/decrypted or authenticated) using the SA before it expires and becomes invalid. The range of permissible values is the set of non-negative integer values between 0 and $2^{32}-1$. The default value is 0 Kilobytes. The value zero specifies the absence of a secured data lifetime.

Note: It is invalid to set both lifetime values to zero! This condition is not enforced by the console (in order to avoid order dependencies when configuring the items), but rather is enforced at runtime and will cause the IPsec profile to assume the defaults.

- **Perfect Forward Secrecy** toggles whether or not Perfect Forward Secrecy will be used. Enabling Perfect Forward Secrecy (the default) causes IKE to perform a new Diffie-Hellman exchange with each Phase 2 re-key. Because the additional Diffie-Hellman exchanges required for Perfect Forward Secrecy introduce additional overhead, it may be good to disable Perfect Forward Secrecy when security does not require it.
- **Dead Peer Detection** toggles whether or not the Router will detect a remote peer being offline.

5-12 Firmware User Guide

- **Maximum Packet Size** permits you to modify the **MTU** setting for the tunnel. Some ISPs require a setting of e.g. 1492 (or other value). The default 1500 is the most common and you usually don't need to change this unless otherwise instructed. Accepted values are from 100 – 1500.

This is the starting value that is used for the MTU when the IPsec tunnel is installed. It specifies the maximum IP packet length for the encapsulated AH or ESP packets sent by the router. The MTU used on the IPsec connection will be automatically adjusted based on the MTU value in any received ICMP *can't fragment* error messages that correspond to IPsec traffic initiated from the router. Normally the MTU only requires manual configuration if the ICMP error messages are blocked or otherwise not received by the router.

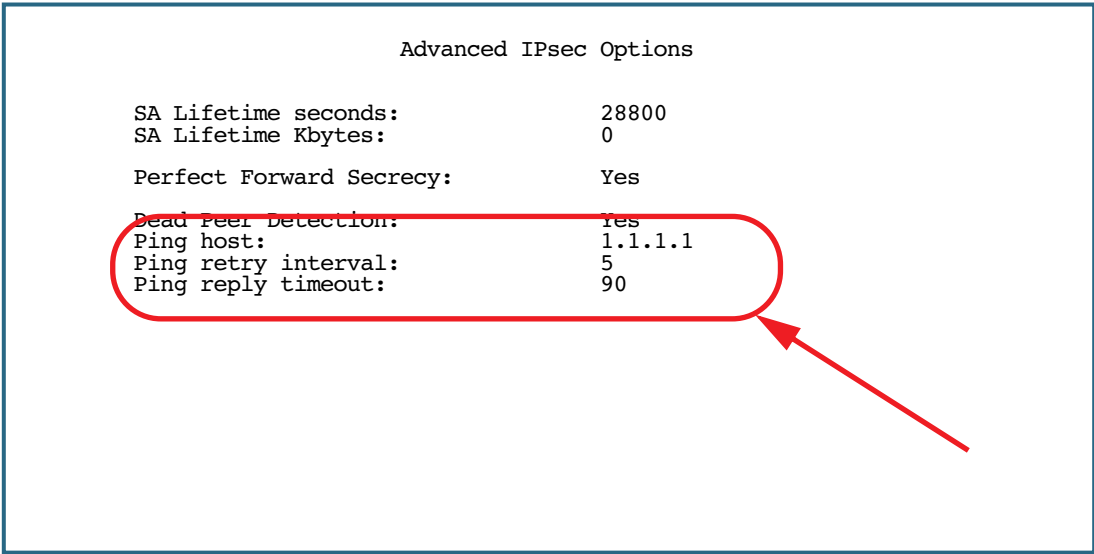
Enhanced Dead Peer Detection

Netopia Firmware Version 8.4 adds a new Dead Peer Detection mechanism.

In previous firmware versions, when Dead Peer Detection was enabled, a counter would begin in the router when any traffic was sent through the tunnel. Determination of a dead peer could take up to eight minutes.

Netopia Firmware Version 8.4 provides a new Dead Peer Detection mechanism. An IPsec IP net interface sends ICMP ping requests to a specific IP address on a Remote Member network. The ping is periodic, and the reply is expected within a certain amount of time. If the ICMP reply does not arrive within that time, the peer is considered dead, the current phase 2 SAs are torn down, and the IKE SA starts a new phase 1 negotiation, followed by the normal phase 2 negotiation, thereafter.

When you toggle **Dead Peer Detection** to **Yes** (on), new options appear.



- **Ping host** allows you to specify the host IP address of the host to ping, and from which replies will be expected.

This field is only available if you have previously configured, and **committed**, remote network IP data in the Add Network Configuration screen under Advanced IP Profile Options. See [“Add Network Configuration” on page 5-14](#).

- **Ping retry interval** and **Ping reply timeout** options appear.

The defaults are 5 seconds and 90 seconds, respectively. You may adjust these to suit your network's tolerances.

Note:

- ICMP Dead Peer Detection is not available when using manual re-keying.
 - ICMP Dead Peer Detection does not initiate a series of phase 2 exchanges upon detecting a dead peer; it instead initiates a new phase 1 negotiation, followed by a new phase 2 negotiation once contact with the peer has been re-established.
 - If you are using Multiple Network IPsec, the IP address of the ICMP Dead Peer Detection mechanism must be constrained to the set of network ranges defined for the IPsec profile.
-

Press Escape to return to the Add or Change Connection Profile screen, and select **IP Profile Parameters**.

If you enable IKE key management the IP Profile Parameters screen appears.

IP Profile Parameters

Remote Tunnel Endpoint: 0.0.0.0

Add Network...

Address Translation Enabled: No

Filter Set... <<None>>

Remove Filter Set

Advanced IP Profile Options...

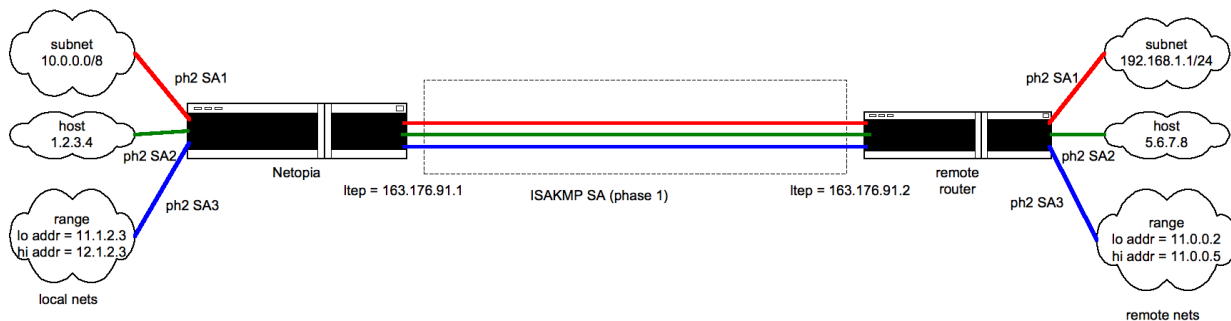
COMMIT CANCEL

- The **Remote Tunnel Endpoint** field accepts either an IP address in the familiar dotted–quad notation a.b.c.d or a hostname to be resolved using the Domain Name System (DNS).

Multiple Network IPsec

Netopia Firmware Version 8.4 offers an enhancement to IPsec VPN tunnels allowing multiple network support. This feature enhances your Netopia Router's Virtual Private Networking functionality.

This feature allows you to define many local and remote network ranges for a given IPsec VPN profile. Each of these ranges has its own IPsec tunnel. However, each tunnel has a common tunneling endpoint and encryption policy. This is useful, for example, for branch office management of multiple IP subnets over an encrypted VPN tunnel. The following diagram illustrates this feature:



Advantages of Multiple Network IPsec are:

- scalability
- flexibility, by adding any combination of remote/local network ranges
- support for sub-netting, host and network range addressing modes
- works with manual keying and Internet Key Exchange (IKE)
- each IPsec network works under the same local/remote tunnel endpoints
- Select **Add Network** and press Return. The Add Network Configuration screen appears.

Add Network Configuration

Remote Member Format...
Remote Member Address:
Remote Member Mask:
Local Member Format...
Local Member Address:
Local Member Mask:

Subnet
Range
Host Address

0.0.0.0
0.0.0.0

COMMIT

CANCEL

- The **Remote Member Format** and **Local Member Format** pop-up menus allow you to choose a format for your network end points: Subnet, Range, or a single Host Address.
 - If you choose **Subnet**, you must enter the **Remote Member Address** and the subnet mask that is the **Remote Member Mask**.
Enter the **Local Member Address** and the **Local Member Mask** in their respective fields.
 - If you choose **Range**, the next two fields become **Remote Member 1st Address** and **Remote Member**

Last Address. You supply these values.

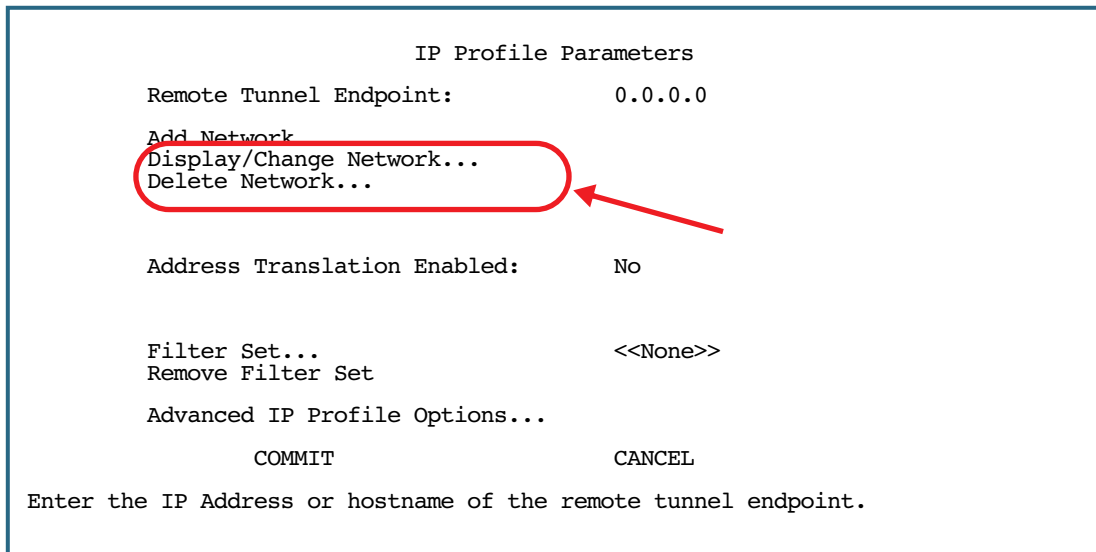
Complete the **Local Member 1st Address** and **Local Member Last Address** fields.

- If you choose **Host Address**, you need only supply the **Remote Member Address** and the **Local Member Address**; the other fields are hidden.
- Select **COMMIT** and press Return to add the configuration. This returns you to the IP Profile Parameters screen. Select **COMMIT** and press Return in the IP Profile Parameters screen. This returns you to the Change Connection Profile screen. Select **COMMIT** and press Return in the Change Connection Profile screen.

Note:

- Any two IPsec tunnels differ only by the local/remote networks they are intended to reach; they have the same encryption policy, which is derived from the base profile.
 - The feature is limited to 8 networks per tunnel.
-

If you return to the IP Profile Parameters screen, two new fields are displayed:



IP Profile Parameters

Remote Tunnel Endpoint:	0.0.0.0
Add Network	
Display/Change Network...	
Delete Network...	
Address Translation Enabled:	No
Filter Set...	<<None>>
Remove Filter Set	
Advanced IP Profile Options...	
COMMIT	CANCEL
Enter the IP Address or hostname of the remote tunnel endpoint.	

- **Display/Change Network** allows you to make changes to existing network configurations you have made. If you select Display/Change Network, a list of your configured networks displays.

```

Display/Change Network Configuration
-----Local-Members-----Remote-Members-----
Net #--Type--Start-Address--Size--Type--Start-Address--Size--
1      SUBNET  192.168.2.1    /24      SUBNET  192.168.1.0    /24
2      SUBNET  10.0.1.1      /8        SUBNET  10.0.0.1      /8
3      HOST    163.176.91.101  -         HOST    163.176.91.100 -
4      RANGE   163.176.30.222  21        RANGE   163.176.91.100 100
-----SCROLL UP-----
-----SCROLL DOWN-----

```

- Scroll down and up with the arrow keys to select the one you want to change, and press Return. You will be returned to the Network Configuration screen where you can make any required changes.
- If you select **Delete Network** in the IP Profile Parameters screen, the same scrolling list will display. When you select one of the networks and press Return, a warning screen will ask you to confirm your choice:

```

1  +-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+24
2  | Are you sure you want to delete this network configuration? |8
3  | CANCEL | CONTINUE | |00
4  +-----+-----+-----+-----+-----+-----+-----+-----+-----+-----+

```

- Specifying IKE key management alters the **Advanced IP Profile Options** screen as follows:

Advanced IP Profile Options

Local Tunnel Endpoint Address:	0.0.0.0
Next Hop Gateway:	0.0.0.0
Idle Timeout (seconds):	300

- You can specify a **Local Tunnel Endpoint Address**. If not 0.0.0.0, this value must be one of the assigned interface addresses, either WAN or LAN. This is used as the source address of all IPsec traffic.
- You can specify a **Next Hop Gateway**. If you specify the Remote Tunnel Endpoint Address, and the address is in the same subnet as the Remote Members Network you specified in the IP Profile Parameters, the **Next Hop Gateway** option allows you to enter the address by which the Router partner is reached.

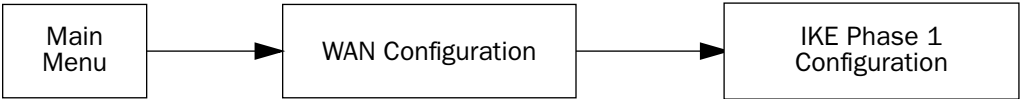
If you do not specify the Remote Tunnel Endpoint Address, the Router will use the default gateway to reach the partner. If the partner should be reached via an alternate port (for example, the LAN instead of the WAN), the **Next Hop Gateway** field allows this path to be resolved.

- You can specify an **Idle Timeout (seconds)** value. The idle timeout tells the Router that if no traffic passes through the tunnel for the specified number of seconds, no automatic SA re-key should be performed. When new traffic does pass through the tunnel, the idle timeout interval resets again when the current SAs expire.

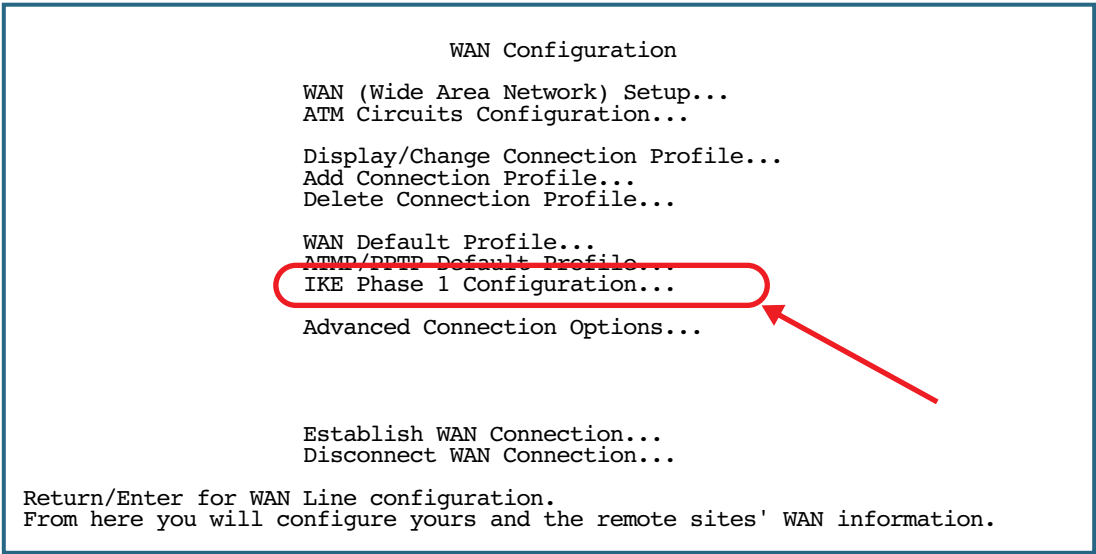
If you set the value to zero, the Router will re-key the SA whenever the SA Lifetime interval specifies, regardless of whether traffic is passing through it or not. This will effectively “nail up” the tunnel.

IPsec WAN Configuration Screens

You can also configure IKE Phase 1 Profiles in the WAN Configuration menus.

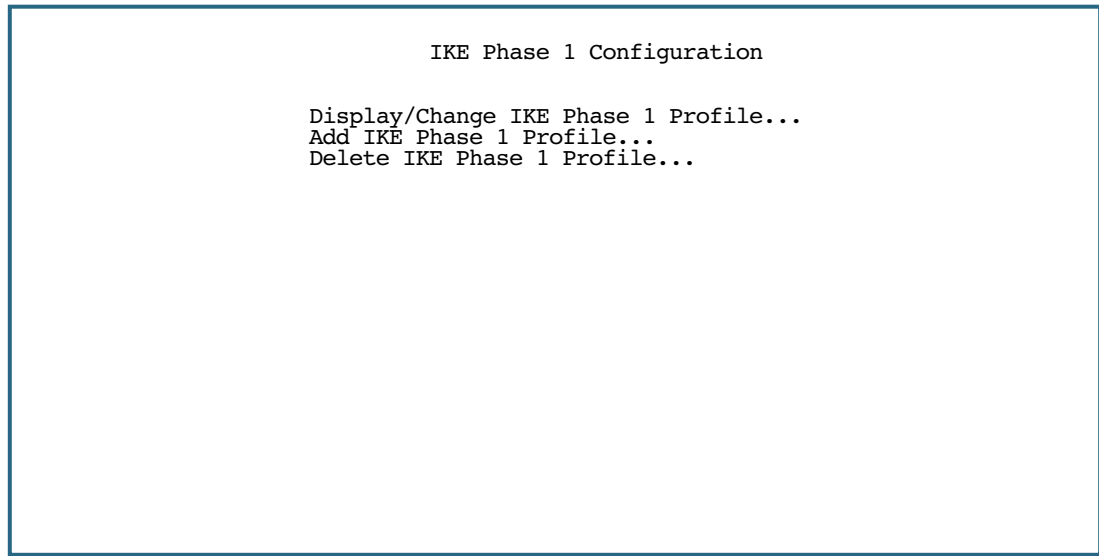


The WAN Configuration screen now includes IKE Phase 1 Configuration as shown:



Select **IKE Phase 1 Configuration** and press Return.

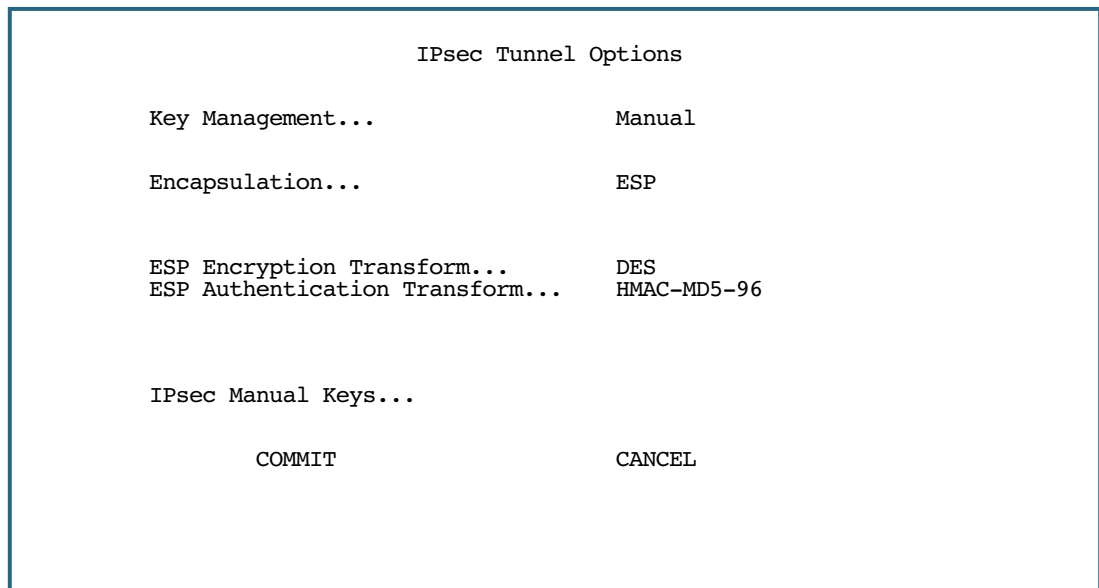
The IKE Phase 1 Configuration screen appears.



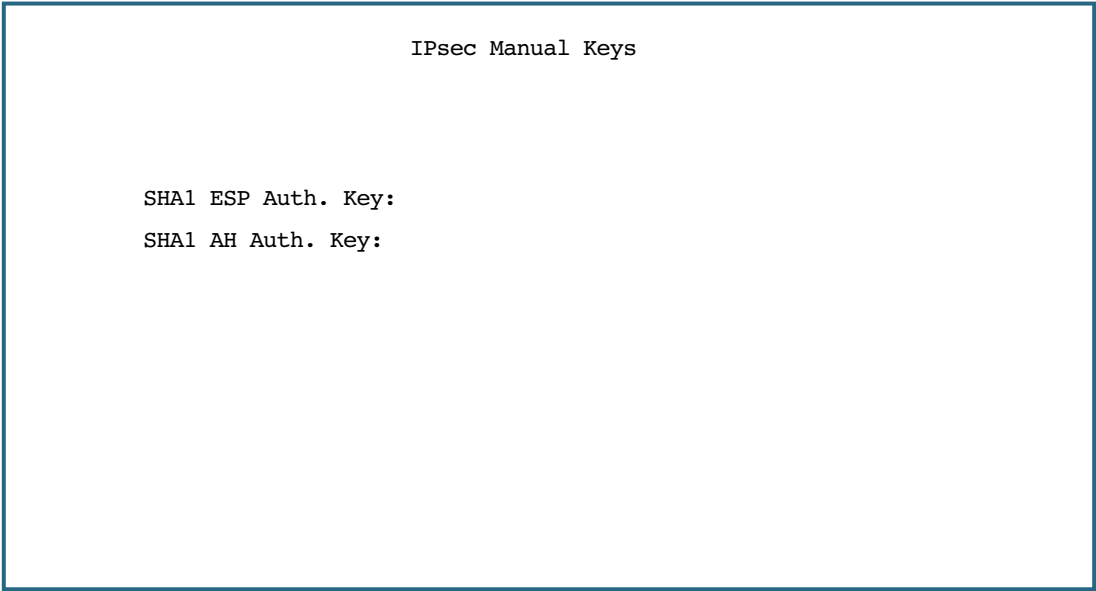
The IKE Phase 1 Configuration screen allows configuration of global (non-connection-profile-specific) IPsec parameters. This screen allows you to Display, Change, Add, or Delete an IKE Phase 1 profile.

IPsec Manual Key Entry

The Version 7.0.2 firmware has a redesigned layout and additional options for manual key entry. If you selected Manual Key Management in the IPsec Tunnel Options screen, you will need to enter your encryption keys in the IPsec Manual Keys screen.



Select **IPsec Manual Keys** and press Return.

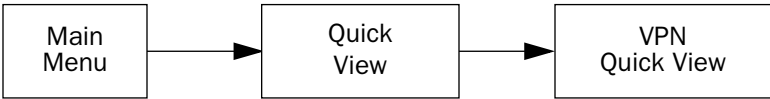


Depending on your selections of Encapsulation, Encryption Transform, and Authentication Transform in the IPsec Tunnel Options screen, the IPsec Manual Keys screen will display differing entry fields to enter authorization keys and encryption keys.

With Manual Keys, you must manually configure identical authentication and encryption keys at both ends of the tunnel. The authentication keys are either 32 (for MD5) or 40 (for SHA1) ascii hex characters, while the encryption keys are 16 (for DES) or 48 (for triple-DES) ascii-hex characters.

VPN Quickview

Statistics are displayed on the VPN Quick View screen.



The VPN Quick View screen has been modified slightly in firmware version 7.0.2.

VPN Quick View						
Profile Name-----	Type--	Rx Pckts--	Tx Pckts--	Discard--	Remote Address--	
HA <-> FA1 (Jony Fon	ATMP	99	99		173.166.82.8	
HA <-> FA3 (Sleve M.	ATMP	13	14		63.193.117.91	
My IPsec Tunnel	IPsec	23	12		0.0.0.0	
Bangalore	PPTP	45	35		1.1.1.1	

If the remote tunnel end point is a hostname (or "0.0.0.0") 0.0.0.0 is displayed until a Security Association is established. Previously the remote members network was displayed.

WAN Event History Error Reporting

The following events are logged and displayed in the WAN Event History screen:

Event message:	Meaning:
IKE: no ph1 preferences assigned	An attempt was made to use an IPsec profile with no IKE profile attached to it.
IKE: DNS lookup failure	The DNS lookup of the remote tunnel end point has failed.
IKE: no matching ph1 profile	An IKE phase 1 request was received and did not match any of the profiles stored in the local Router.
IKE: no matching proposal	An IKE phase 1 request was received and the proposal did not match an allowed parameter, or else the remote rejected the local Router's proposal.
IKE: phase 1 auth failure	The phase 1 remote authentication failed.
IKE: phase 1 resend timeout	The attempt to resend the phase 1 remote authentication timed out.
IKE: phase 1 complete	The phase 1 negotiation completed successfully.
IKE: phase 2 hash failure	The phase-2 hash failed because the data received is out of date or has been tampered with.

Event message:	Meaning:
IKE: no matching ph2 proposal	Either the local Router rejected the proposals of the remote or the remote rejected the local Router's.
IKE: ph2 resend timeout	The attempt to resend the phase 2 authentication timed out.
IKE: phase 2 complete	The phase 2 negotiation completed successfully.

Chapter 6

IP Setup

The Netopia Firmware Version 8.4 uses Internet Protocol (IP) to communicate both locally and with remote networks. This chapter shows you how to configure the gateway to route IP traffic. You also learn how to configure the gateway to serve IP addresses to hosts on your local network.

Netopia's IP routing features Network Address Translation and IP address serving.

This section covers the following topics:

- [“IP Setup” on page 6-2](#)
- [“RIP-2 MD5 Authentication” on page 6-10](#)
- [“IP Address Serving” on page 6-17](#)
- [“More Address Serving Options” on page 6-23](#)
- [“DHCP Relay Agent” on page 6-28](#)
- [“Connection Profiles” on page 6-30](#)
- [“Multicast Forwarding” on page 6-33](#)

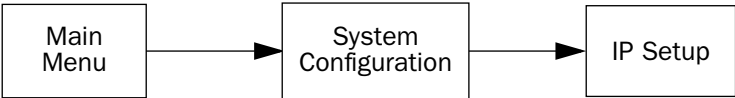
Network Address Translation allows communication between the LAN connected to the Router and the Internet using a single (or a few) IP address(es) instead of a routed account with separate IP addresses for each computer on the network.

Network Address Translation also provides increased security by hiding the local IP addresses of the LAN connected to the Netopia gateways from the outside world.

The setup is simpler, so ISPs typically offer Internet accounts supporting Network Address Translation at a significant cost savings.

For a detailed discussion of Network Address Translation, see [Chapter 3, “Multiple Network Address Translation.”](#)

IP Setup



The IP Setup options screen is where you configure the Ethernet side of the Router. The information you enter here controls how the gateway routes IP traffic.

Consult your network administrator or ISP to obtain the IP setup information (such as the Ethernet IP address, Ethernet subnet mask, default IP gateway, and Primary Domain Name Server IP address) you will need before changing any of the settings in this screen. Changes to these settings that you make in this screen will take effect only after the Netopia device is reset.

To go to the IP Setup options screen, from the Main Menu, select **System Configuration**, then **IP Setup**.

The IP Setup screen appears.

IP Setup

Ethernet IP Address:	192.128.117.162
Ethernet Subnet Mask:	255.255.255.0
Define Additional Subnets...	
Default IP Gateway:	192.128.117.163
Backup IP Gateway:	0.0.0.0
Primary Domain Name Server:	0.0.0.0
Secondary Domain Name Server:	0.0.0.0
Domain Name:	yourdomain.com
Receive RIP...	Both
Transmit RIP...	Off
Multicast Forwarding...	None
Static Routes...	IP Address Serving...

Follow these steps to configure IP setup for your Router:

- Select **Ethernet IP Address** and enter the IP address for the Router’s Ethernet port.
- Select **Ethernet Subnet Mask** and enter the subnet mask for the Ethernet IP address that you entered in the last step.
- If you desire multiple subnets select **Define Additional Subnets**. If you select this item you will be taken to the IP Subnets screen. This screen allows you to define IP addresses and masks for additional subnets. See [“IP subnets” on page 6-4](#) for details.

The Netopia Firmware Version 8.4 supports multiple IP subnets on the Ethernet interface. You may want to configure multiple IP subnets to service more hosts than are possible with your primary subnet. It is not always possible to obtain a larger subnet from your ISP. For example, if you already have a full Class C subnet, your only option is multiple Class C subnets, since it is virtually impossible to justify a Class A or Class B assignment.

If you are using NAT, you can use the reserved Class A or Class B subnet.

- Select **Default IP Gateway** and enter the IP address for a default gateway. This can be the address of any major gateway accessible to the Router.

A default gateway should be able to successfully route packets when the Router doesn't know how to route to the intended recipient's IP address. Typically, a default gateway is the ISP's gateway.

- If a backup gateway is available, select **Backup IP Gateway** and enter the IP address of a gateway that you want to use for backup in the event of a connection failure. See [“Backup Default Gateway” on page 7-14](#) for configuration details.
 - Select **Primary Domain Name Server** and enter the IP address for a domain name server. The domain name server matches the alphabetic addresses favored by people (for example, robin.hood.com) to the IP addresses actually used by IP gateways (for example, 163.7.8.202).
 - If a secondary DNS server is available, select **Secondary Domain Name Server** and enter its IP address. The secondary DNS server is used by the Router when the primary DNS server is inaccessible. Entering a secondary DNS is useful but not necessary.
 - Select **Domain Name** and enter your network's domain name (for example, netopia.com). Netopia strongly recommends that you enter a domain name.
- n** Routing Information Protocol (RIP) is needed if there are IP routers on other segments of your Ethernet network that the Router needs to recognize. If this is the case select **RIP Options** and press Return. This will take you to the Ethernet LAN RIP options screen, where you can configure several parameters, including RIP v2 MD5 Authentication. See [“RIP-2 MD5 Authentication” on page 6-10](#).
- n** With Receive RIP set to v1, the Ethernet port will accept routing information provided by RIP packets from other routers that use the same subnet mask. Set to v2, the router will accept routing information provided by RIP packets from other routers that use different subnet masks. Set to Both, the router will accept information from either RIP v1 or v2 routers.
 - n** With Transmit RIP v1 selected, the router will generate RIP packets only to other RIP v1 routers. With Transmit RIP v2 (broadcast) selected, the router will generate RIP packets to all other hosts on the network. With Transmit RIP v2 (multicast) selected, the router will generate RIP packets only to other routers capable of recognizing RIP v2 packets.
- If you want to enable Multicast Forwarding, select **Multicast Forwarding** and from the pop-up menu, choose the type that you want to enable. See [“Multicast Forwarding” on page 6-33](#) for detailed configuration.
- If you enable Multicast Forwarding, the next field **IGMP Version** appears. You can choose v1 or v2 from the pop-up menu.
- Select **Static Routes** to manually configure IP routes. See the section [“Static routes,”](#) below.
 - If you select **IP Address Serving** you will be taken to the IP Address Serving screen (see [“IP Address Serving” on page 6-17](#)). Since no two hosts can use the same IP address at the same time, make sure

that the addresses distributed by the Router and those that are manually configured are not the same. Each method of distribution must have its own exclusive range of addresses to draw from.

IP subnets

The IP Subnets screen allows you to configure up to eight Ethernet IP subnets on unlimited-user models, one “primary” subnet and up to seven secondary subnets, by entering IP address/subnet mask pairs:

IP Subnets

	IP Address	Subnet Mask
#1:	192.128.117.162	255.255.255.0
#2:	0.0.0.0	0.0.0.0
#3:		
#4:		
#5:		
#6:		
#7:		
#8:		

Note: You need not use this screen if you have only a single Ethernet IP subnet. In that case, you can continue to enter or edit the IP address and subnet mask for the single subnet on the IP Setup screen.

This screen displays up to eight rows of two editable columns, preceded by a row number between one and eight. If you have eight subnets configured, there will be eight rows on this screen. Otherwise, there will be one more row than the number of configured subnets. The last row will have the value 0.0.0.0 in both the IP address and subnet mask fields to indicate that you can edit the values in this row to configure an additional subnet. All eight row labels are always visible, regardless of the number of subnets configured.

- To add an IP subnet, enter the Router’s IP address on the subnet in the **IP Address** field in a particular row and the subnet mask for the subnet in the **Subnet Mask** field in that row.

For example:

IP Subnets		
	IP Address	Subnet Mask
	-----	-----
#1:	192.128.117.162	255.255.255.0
#2:	192.128.152.162	255.255.0.0
#3:	0.0.0.0	0.0.0.0
#4:		
#5:		
#6:		
#7:		
#8:		

- To delete a configured subnet, set both the IP address and subnet mask values to 0.0.0.0, either explicitly or by clearing each field and pressing Return to commit the change. When a configured subnet is deleted, the values in subsequent rows adjust up to fill the vacant fields.

The subnets configured on this screen are tied to the address serving pools configured on the IP Address Pools screen, and that changes on this screen may affect the IP Address Pools screen. In particular, deleting a subnet configured on this screen will delete the corresponding address serving pool, if any, on the IP Address Pools screen.

If you have configured multiple Ethernet IP subnets, the IP Setup screen changes slightly:

IP Setup

Subnet Configuration...

Default IP Gateway:	192.128.117.163
Primary Domain Name Server:	0.0.0.0
Secondary Domain Name Server:	0.0.0.0
Domain Name:	
Receive RIP...	Both
Transmit RIP...	v2 (multicast)

Static Routes...IP Address Serving...

Network Address Translation (NAT)...

Set up the basic IP attributes of your Netopia in this screen.

The IP address and Subnet mask items are hidden, and the **Define Additional Subnets...** item becomes **Subnet Configuration...**. If you select **Subnet Configuration**, you will return to the IP Subnets screen that allows you to define IP addresses and masks for additional Ethernet IP subnets.

Static routes

Static routes are IP routes that are maintained manually. Each static route acts as a pointer that tells the Router how to reach a particular network. However, static routes are used only if they appear in the IP routing table, which contains all of the routes used by the Router (see [“IP Routing Table” on page 8-7](#)).

Static routes are helpful in situations where a route to a network must be used and other means of finding the route are unavailable. For example, static routes are useful when you cannot rely on RIP.

To go to the Static Routes screen, select **Static Routes** in the IP Setup screen and press Return.

The Static Routes screen will appear.

Static Routes

Display/Change Static Route...

Add Static Route...

Delete Static Route...

Configure/View/Delete Static Routes from this and the following Screens.

Viewing static routes

To display a view-only table of static routes, select **Display/Change Static Route**. The table shown below will appear.

+-Dest. Network	---Subnet Mask----	Next Gateway----	Priority	Enabled--+
0.0.0.0	0.0.0.0	163.176.8.1	Low	Yes

Select a Static Route to modify.

The table has the following columns:

Dest. Network: The network IP address of the destination network.

Subnet Mask: The subnet mask associated with the destination network.

Next Gateway: The IP address of the gateway that will be used to reach the destination network.

Priority: An indication of whether the Router will use the static route when it conflicts with information received from RIP packets.

Enabled: An indication of whether the static route should be installed in the IP routing table.

To return to the Static Routes screen, press Escape.

Adding a static route

To add a new static route, select **Add Static Route** in the Static Routes screen. The Add Static Route screen will appear.

Add Static Route

Static Route Enabled:	Yes
Destination Network IP Address:	0.0.0.0
Destination Network Subnet Mask:	0.0.0.0
Next Gateway IP Address:	0.0.0.0
Route Priority...	High
Advertise Route Via RIP:	No

ADD STATIC ROUTE NOW

CANCEL

Configure a new Static Route in this Screen.

- To install the static route in the IP routing table, select **Static Route Enabled** and toggle it to **Yes**. To remove the static route from the IP routing table, select **Static Route Enabled** and toggle it to **No**.
- Be sure to read the rules on the installation of static routes in the IP routing table. See [“Rules of static route installation” on page 6-9](#).
- Select **Destination Network IP Address** and enter the network IP address of the destination network.
- Select **Destination Network Subnet Mask** and enter the subnet mask used by the destination network.
- Select **Next Gateway IP Address** and enter the IP address for the gateway that the Router will use to reach the destination network. This gateway does not necessarily have to be part of the destination network, but it must at least know where to forward packets destined for that network.
- Select **Route Priority** and choose **High** or **Low**. High means that the static route takes precedence over RIP information; Low means that the RIP information takes precedence over the static route.
- If the static route conflicts with a connection profile, the connection profile will always take precedence.

- To make sure that the static route is known only to the Router, select **Advertise Route Via RIP** and toggle it to **No**. To allow other RIP-capable gateways to know about the static route, select **Advertise Route Via RIP** and toggle it to **Yes**. When Advertise Route Via RIP is toggled to **Yes**, a new item called **RIP Metric** appears below **Advertise Route Via RIP**.

With RIP Metric you set the number of gateways, from 1 to 15, between the sending gateway and the destination gateway. The maximum number of gateways on a packet's route is 15. Setting **RIP Metric** to **1** means that a route can involve 15 gateways, while setting it to **15** means a route can only involve one gateway.

- Select **ADD STATIC ROUTE NOW** to save the new static route, or select **CANCEL** to discard it and return to the Static Routes screen.
- Up to 32 static routes can be created, but one is always reserved for the default gateway, which is configured using either Easy Setup or the IP Setup screen in system configuration.

Modifying a static route

To modify a static route, in the Static Routes screen select **Display/Change Static Route** to display a table of static routes.

Select a static route from the table and go to the Change Static Route screen. The parameters in this screen are the same as the ones in the Add Static Route screen (see [“Adding a static route” on page 6-8](#)).

Deleting a static route

To delete a static route, in the Static Routes screen select **Delete Static Route** to display a table of static routes. Select a static route from the table and press Return to delete it. To exit the table without deleting the selected static route, press Escape.

Rules of static route installation

The Netopia Firmware Version 8.4 applies certain rules before installing enabled static routes in the IP routing table. An enabled static route will not be installed in the IP routing table if any of the following conditions are true:

- The static route's **Next Gateway IP Address** matches an IP address in the range of IP addresses being distributed by DHCP.
- The static route's **Next Gateway IP Address** is determined to be unreachable by the Router.
- The static route's route information conflicts with a connection profile's route information.
- The connection profile associated with the static route has a disabled dial-on-demand setting, and there is no current connection using that connection profile.

A static route that is already installed in the IP routing table will be removed if any of the conditions listed above become true for that static route. However, an enabled static route is automatically reinstalled once the conditions listed above are no longer true for that static route.

RIP-2 MD5 Authentication

Firmware version 5.3.7 supports RIP-2 MD5 Authentication (RFC2082 Routing Internet Protocol Version 2, Message Digest 5). The purpose of MD5 authentication is to provide an additional level of confidence that a RIP packet received was generated by a reliable source. In other words, MD5 authentication provides an enhanced level of security that information that your PC receives does not originate from a malicious source posing as part of your network.

Overview

All participants in an authenticated RIP environment on a network must share an identifier key. There is no key exchange protocol like IKE, so all keys must be manually entered by an administrator.

RIP-2 MD5 Authentication requires that an interface configured to receive authenticated packets ignore unauthenticated packets or packets authenticated with an invalid key. An interface that is not configured for receiving authenticated packets ignores authenticated ones.

On a Netopia router, every interface will be allowed to have up to two keys. RIP-2 MD5 authentication can be configured on the Ethernet LAN (all models), Ethernet WAN models, Connection Profiles, and the Default Profile. Keys can have lifetimes, defined as a start date and time and an end date and time, or infinite.

Key management

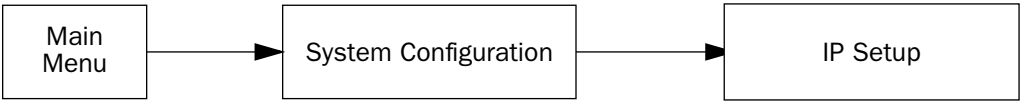
Typically, you configure only one key on a given interface and all of the interfaces that interact with that interface. RIP updates are sent every 30 seconds. Each RIP packet is authenticated using one key and sent. When the Netopia router receives an authenticated RIP packet from a device, it keeps track of that device (peer).

The longer it is in use, a single key becomes less secure. Therefore, RFC2082 specifies that an interface *must* support at least two keys per interface to allow a transition from an old key to a new key. It is recommended that you specify an overlapping time of five minutes for transitioning from one key to the next. Whenever two keys are valid at the same time, the Netopia router tries to determine if other peers (devices that it has received an authenticated packet from in the past three minutes) on its network are using the new key. If any of the peers have not used the new key yet, the Netopia router will send RIP updates twice, once with each key.

If the last valid key expires, the Device Event History logs a “* RIP: last authentication key expired” message, and continues to use that key as if it were still valid.

Authentication configuration

To configure RIP-2 MD5 authentication, from the Main Menu, select **System Configuration**, then **IP Setup**.



The IP Setup screen appears.

IP Setup

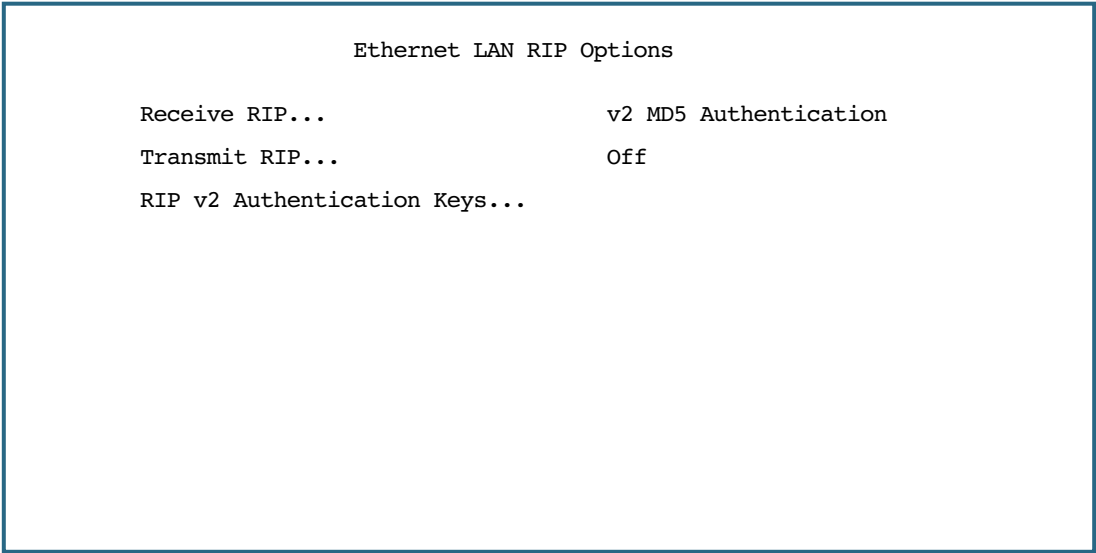
Ethernet IP Address:	192.168.1.1
Ethernet Subnet Mask:	255.255.255.0
Define Additional Subnets...	
Default IP Gateway:	0.0.0.0
Backup IP Gateway:	0.0.0.0
Primary Domain Name Server:	0.0.0.0
Secondary Domain Name Server:	0.0.0.0
Domain Name:	
RIP Options...	
Multicast Forwarding...	None
Static Routes...	IP Address Serving...

- Select **RIP Options**. The Ethernet LAN RIP Options screen appears.

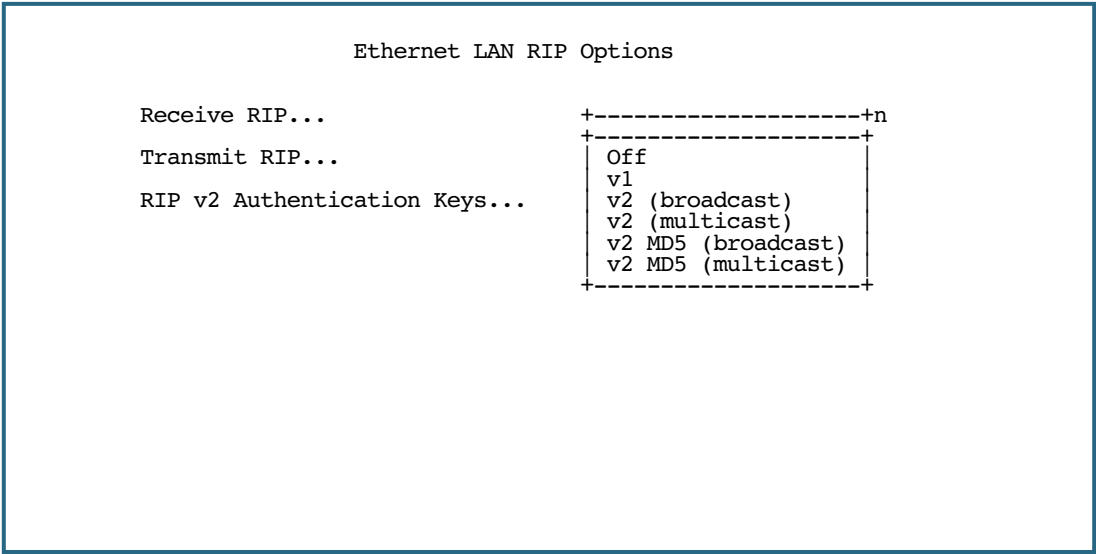
Ethernet LAN RIP Options

Receive RIP...	Off
Transmit RIP...	v1
	v2
	Both v1 and v2
	v2 MD5 Authentication

- Select **Receive RIP**, and from the pull-down menu choose **v2 MD5 Authentication**.



- You can also select **Transmit RIP**, and choose **v2 MD5 (broadcast)** or **v2 MD5 (multicast)** from the pull-down menu.



- **RIP v2 Authentication Keys** is visible only if v2 MD5 Authentication is enabled for either Receive or Transmit RIP.

Note:

- All of the changes on this menu require a reboot. This is unique to the Ethernet LAN. RIP changes on all other interfaces are immediately effective.
- If you set the RIP Receive option to **Both v1 and v2**, the interface will ignore authenticated RIP packets since authenticated v1 packets do not exist. Only v2 packets can be authenticated.

- Select **RIP v2 Authentication Keys**.

The RIP v2 Authentication Keys screen appears.

RIP v2 Authentication Keys

Display/Change Key...

Add Key...

Delete Key...

Adding a key

Select **Add Key**. The Add Key Screen appears.

Add Key

Key ID:	0
Authentication Key:	
Start Date (MM/DD/YY):	10/10/2002
Start Time (hh:mm):	12:00
AM or PM:	AM
End Time Mode:	Date
End Date (MM/DD/YY):	10/10/2002
End Time (hh:mm):	12:00
AM or PM:	AM
<div style="display: inline-block; width: 45%;">COMMIT</div> <div style="display: inline-block; width: 45%;">CANCEL</div>	

- The key identifier **Key ID** can be any numeric value from 0 – 255, and must be unique per interface. You can not have two keys with the same key ID on an interface.
- The **Authentication Key** may consist of from 1 – 16 ASCII characters. These appear as asterisks when typed.

6-14 Firmware User Guide

- The **Start Date** and **End Date** formats are determined by the System Date Format, set on the Set Date and Time menu under the System Configuration menus.
- The **Start Time** and **End Time** formats are determined by the System Time Format. The AM or PM pull-down menus do not appear if the time format is 24 hour time.
- The **End Time Mode** pull-down menu allows you to select either Date or Infinite. This determines whether or not the key will expire at a specified time and date, or remain effective indefinitely.

End Date, **End Time**, and **AM or PM** do not appear if the End Time Mode is set to “Infinite”. Infinite means that the key begins when it begins, but it never expires. The acceptable year range is from 1904 – 2039.

- When you are satisfied with your entries, select **COMMIT** and press Return.

This menu will not accept a non-unique Key ID on the same interface; failure to enter an authentication key; or a negative start date, end date, or start time and end time range.

Changes to RIP Keys on all interfaces are immediately effective. This differs from the remainder of the RIP configuration on the Ethernet LAN, which requires a reboot. It is important that the keys be able to change dynamically, however, because the purpose of entering more than one key on an interface is to insure a smooth transition between keys with no network outages.

Changing or deleting a key

You change or delete a key by selecting it from a pop-up menu. In the RIP v2 Authentication Keys menu, select **Display/Change Key**.

RIP v2 Authentication Keys

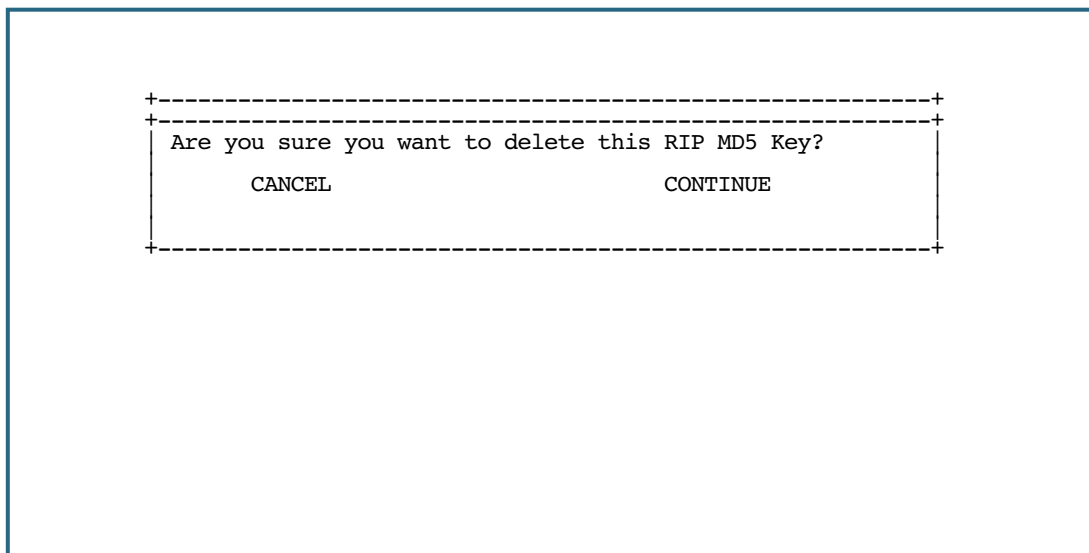
+Key ID	--Start Date	--Start Time	--End Date	--End Time	--Valid	+
1	10/10/2002	12:00 AM	Infinite		yes	
255	3/11/2000	3:17 PM	8/6/2002	1:24 AM	no	

Delete Key...

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

Note: The date and time formats are determined by the system date and time formats. If the current date and time fall within the range of dates and times, the **Valid** field indicates “yes”, otherwise it indicates “no”.

You modify the **Change Key** menu in the same way as in the Add Key menu (see [“Adding a key,” on page 13](#)). If you select **Delete Key**, a pop-up menu will ask you to confirm your choice.

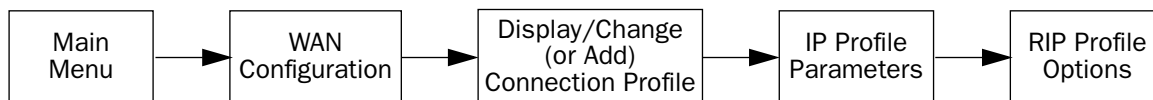


Connection Profiles and Default Profile

RIP-2 MD5 authentication may be configured in Connection Profiles, as well. If you are not using NAT, your public Internet connection can benefit from sending authenticated RIP packets as well as receiving them. To configure RIP-2 MD5 authentication for a Connection Profile, you can either change an existing Connection Profile, or create a new one.

The Default Profile Leased and Switched menus are the same as the Connection Profile RIP option and associated menus. For brevity, the following example shows only the Connection Profile RIP option and associated menus.

In either case, navigate to the **RIP Profile Parameters** screen under the IP Profile Parameters menu of the Display/Change (or Add) Connection Profile screen.



The connection profile RIP Profile Parameters screen appears.

RIP Profile Parameters

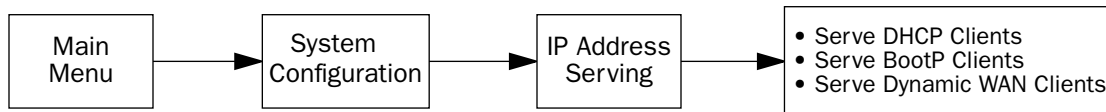
Receive RIP:	v2 MD5 Authentication
Transmit RIP:	v2 MD5 (multicast)
TX RIP Policy...	Poison Reverse
RIP v2 Authentication Keys...	

- **Receive RIP** is always visible. Here you select Off, v1, v2, Both v1 and v2, or v2 MD5 Authentication from the pull-down menu. For MD5 authentication, you must select **v2 MD5 Authentication**.
- If NAT is disabled, **Transmit RIP** is visible. Here you select Off, v1, v2 (broadcast), v2 (multicast), v2 MD5 (broadcast), or v2 MD5 (multicast) from the pull-down menu. For MD5 authentication, you must select **v2 MD5** (either **broadcast** or **multicast**).
- If you chose any Transmit RIP option other than Off, **TX RIP Policy** is visible. Here you select Poison Reverse, Split Horizon, or No Split Horizon from the pull-down menu. Unless otherwise instructed, leave the default Poison Reverse.
- If either Receive RIP or Transmit RIP is set to v2 MD5 Authentication, **RIP v2 Authentication Keys** is visible. Selecting RIP v2 Authentication Keys takes you to the RIP v2 Authentication Keys screen, where you can configure your keys in the same manner as in [“Adding a key,” on page 13](#). After configuring your key, press **COMMIT** in the Add or Change Key screen, then press Escape three times to return to the Add or Change Connection Profile screen.
- Select **COMMIT** in the Connection Profile screen and press Return. Your changes become effective for the specified Connection Profile.

Power interruptions

Netopia 4000 Series routers use NTP updates to set the correct time. Consequently, the starting time after a power cycle, whether from power failure or deliberately switching power off and on, is in the year 1904. This could invalidate some keys that would otherwise be valid. To prevent this, if the system time is before the year 2000, all keys are considered valid regardless of their specified date and time ranges.

IP Address Serving



In addition to being a gateway, the Router is also an IP address server. There are three protocols it can use to distribute IP addresses.

- The first, called Dynamic Host Configuration Protocol (DHCP), is widely supported on PC networks, as well as Apple Macintosh computers using Open Transport and computers using the UNIX operating system. Addresses assigned via DHCP are “leased” or allocated for a short period of time; if a lease is not renewed, the address becomes available for use by another computer. DHCP also allows most of the IP parameters for a computer to be configured by the DHCP server, simplifying setup of each machine.
- The second, called BootP (also known as Bootstrap Protocol), is the predecessor to DHCP and allows older IP hosts to obtain most of the information that a DHCP client would obtain. However, in contrast, BootP address assignments are “permanent” since there is no lease renewal mechanism in BootP.
- The third protocol, called Dynamic WAN, is part of the PPP/MP suite of wide area protocols used for WAN connections. It allows remote terminal adapters and NAT-enabled gateways to be assigned a temporary IP address for the duration of their connection.

Since no two hosts can use the same IP address at the same time, make sure that the addresses distributed by the Router and those that are manually configured are not the same. Each method of distribution must have its own exclusive range of addresses to draw from.

Go to the System Configuration screen. Select **IP Address Serving** and press Return. The IP Address Serving screen will appear.

IP Address Serving	
IP Address Serving Mode...	<div style="border: 1px dashed black; padding: 2px;"> Disabled DHCP Server DHCP Relay Agent </div>
Number of Client IP Addresses:	
1st Client Address:	
Client Default Gateway...	192.168.1.1
Serve DHCP Clients:	Yes
DHCP Lease Time (Hours):	1
DHCP NetBIOS Options...	
Serve BOOTP Clients:	Yes
Serve Dynamic WAN Clients	Yes

Follow these steps to configure IP Address Serving:

- If you enabled IP Address Serving, then DHCP, BootP clients and Dynamic WAN clients are automatically enabled.
- The **IP Address Serving Mode** pop-up menu allows you to choose the way in which the Router will serve IP addresses. The device can act as either a DHCP Server or a DHCP Relay Agent. (See [“DHCP Relay Agent” on page 6-28](#) for more information.) In most cases, you will use the device to serve its own pool of IP addresses, hence DHCP Server is the default. Address serving can also be disabled.
- Select **Number of Client IP Addresses** and enter the total number of contiguous IP addresses that the Router will distribute to the client machines on your local area network. Twelve-user models are limited to twelve IP addresses.

In the screen example shown above, five Client IP addresses have been allocated.

- Select **1st Client Address** and enter the first client IP address that you will allocate to your first client machine. For instance, on your local area network you may want to first figure out which machines are going to be allocated specific static IP addresses so that you can determine the pool of IP addresses that you will be serving addresses from via DHCP, BootP, and/or Dynamic WAN.

Example: Your ISP has given your Router the IP address 192.168.6.137, with a subnet mask of 255.255.255.248. The subnet mask allocated will give you six IP addresses to use when connecting to the ISP over the Internet. Your address range will be from **.137 – .143**. In this example you would enter **192.168.6.138** as the 1st Client Address, since the gateway itself must have an IP address.

- To enable DHCP, select **Serve DHCP Clients** and toggle it to **Yes**. DHCP serving is automatic when IP Address Serving is enabled.
- The default DHCP Lease time is one hour. This may be unnecessarily brief in your network environment. Consequently, the DHCP lease time is configurable. The **DHCP Lease Time (Hours)** setting allows you to modify the gateway's default lease time of one hour. You can enter any number up to and including 168 hours (one week) for the DHCP lease.

Note: About DHCP Auto-configuration:

Certain model gateways whose model number ends in will allow the IP Address Server to auto-configure when the gateway is configured with a new IP Address and Subnet Mask. This applies according to the following guidelines:

- If you configure the gateway with a 24 bit Subnet Mask (Class C), the gateway will continue serving from 100-199, with the new IP Address.
 - If you configure the gateway with a subnet smaller than a Class C subnet, the gateway will serve all available addresses.
 - If you explicitly configure the DHCP pool, auto-configuration of the DHCP pool is suppressed.
 - If you configure the gateway manually and you would like the gateway to auto-configure DHCP, you must explicitly set the IP Address and Subnet Mask to 0.0.0.0 and reboot.
-

If you have configured multiple Ethernet IP subnets, the appearance of the IP Address Serving screen is altered slightly:

IP Address Serving	
IP Address Serving Mode...	DHCP Server
Configure Address Pools...	
Serve DHCP Clients:	Yes
DHCP Lease Time (Hours):	1
DHCP NetBIOS Options...	
Serve BOOTP Clients:	Yes
Serve Dynamic WAN Clients	Yes

Three menu items are hidden, and **Configure Address Pools...** appears instead. If you select **Configure Address Pools...** you will be taken to the IP Address Pools screen that allows you to configure an address serving pool for each of the configured Ethernet IP subnets. See [“IP Address Pools” on page 6-20](#).

IP Address Pools

The IP Address Pools screen allows you to configure a separate IP address serving pool for each of up to eight configured Ethernet IP subnets:

IP Address Pools			
Subnet (# host addrs)	1st Client Addr	Clients	Client Gateway
192.128.117.0 (253)	192.128.117.196	16	192.128.117.162
192.129.117.0 (253)	192.129.117.110	8	192.129.117.4

This screen consists of between two and eight rows of four columns each. There are exactly as many rows as there are Ethernet IP subnets configured on the IP Subnets screen.

- The **Subnet (# host addrs)** column is non-selectable and non-editable. It indicates the network address of the Ethernet IP subnet for which an address pool is being configured and the number of host addresses available on the subnet. The network address is equal to the gateway’s IP address on the subnet bitwise-ANDed with the subnet mask. The host address count is equal to the subnet size minus three, since one address is reserved for the network address, one for the subnet broadcast address, and one for the gateway’s interface address on the subnet.

You can edit the remaining columns in each row.

- The **1st Client Addr** and **Clients** columns allow you to specify the base and extent of the address serving pool for a particular subnet. Entering 0.0.0.0 for the first client address or 0 for the number of clients indicates that no addresses will be served from the corresponding Ethernet IP subnet.
- The Client Gateway column allows you to specify the default gateway address that will be provided to clients served an address from the corresponding pool. The value defaults to the Router’s IP address on the corresponding subnet (or the Router’s default gateway, if that gateway is located on the subnet in question). You can override the value by entering any address that is part of the subnet.

DHCP, BootP, and dynamic WAN clients may receive an address from any one of the address serving pools configured on this screen.

Numerous factors influence the choice of served address. It is difficult to specify the address that will be served to a particular client in all circumstances. However, when the address server has been configured, and the clients involved have no prior address serving interactions, the Router will generally serve the first unused address from the first address pool with an available address. The Router starts from the pool on the first row and continues to the pool on the last row of this screen.

Once the address server and/or the clients have participated in address serving transactions, different rules apply:

- When requesting an address, a client will often suggest an address to be assigned, such as the one it was last served. The Router will attempt to honor this request if the address is available. The client stores this address in non-volatile storage, for example, on disk, and the specific storage method/location differs depending on the client operating system.
- When requesting an address, a client may provide a client identifier, or, if it does not, the Netopia Firmware Version 8.4 may construct a pseudo-client identifier for the client. When the client subsequently requests an address, the Router will attempt to serve the address previously associated with the pseudo-client identifier. This is normally the last address served to the client.
- Otherwise, the Netopia will select the least-recently used available address, starting from the first address in the first pool and ending with the last address in the last pool.

Note: The address serving pools on this screen are tied to the IP subnets configured on the IP Subnets screen. Changes to the IP Subnets screen may affect this screen. In particular, deleting a subnet on the IP Subnets screen will delete the corresponding address serving pool, if any, on this screen.

DHCP NetBIOS Options

If your network uses NetBIOS, you can enable the Router to use DHCP to distribute NetBIOS information.

NetBIOS stands for Network Basic Input/Output System. It is a layer of software originally developed by IBM and Sytek to link a network operating system with specific hardware. NetBIOS has been adopted as an industry standard. It offers LAN applications a variety of “hooks” to carry out inter-application communications and data transfer. Essentially, NetBIOS is a way for application programs to talk to the network. To run an application that works with NetBIOS, a non-IBM network operating system or network interface card must offer a NetBIOS emulator. Many vendors either provide a version of NetBIOS to interface with their hardware or emulate its transport layer communications services in their network products. A NetBIOS emulator is a program provided by NetWare clients that allow workstations to run applications that support IBM’s NetBIOS calls.

- Select **DHCP NetBIOS Options** and press Return. The DHCP NetBIOS Options screen appears.

DHCP NetBIOS Options

Serve NetBIOS Type:	Yes
NetBIOS Type...	Type B
Serve NetBIOS Scope:	No
NetBIOS Scope:	
Serve NetBIOS Name Server:	No
NetBIOS Name Server IP Addr:	0.0.0.0

Configure DHCP-served NetBIOS options here.

- To serve DHCP clients with the type of NetBIOS used on your network, select **Serve NetBIOS Type** and toggle it to **Yes**.
- From the **NetBIOS Type** pop-up menu, select the type of NetBIOS used on your network.

DHCP NetBIOS Options

Serve NetBIOS Type:	+-----+
NetBIOS Type...	+-----+
	Type B
	Type P
	Type M
	Type H
	+-----+
Serve NetBIOS Scope:	No
NetBIOS Scope:	
Serve NetBIOS Name Server:	No
NetBIOS Name Server IP Addr:	0.0.0.0

Local network Broadcast nodes

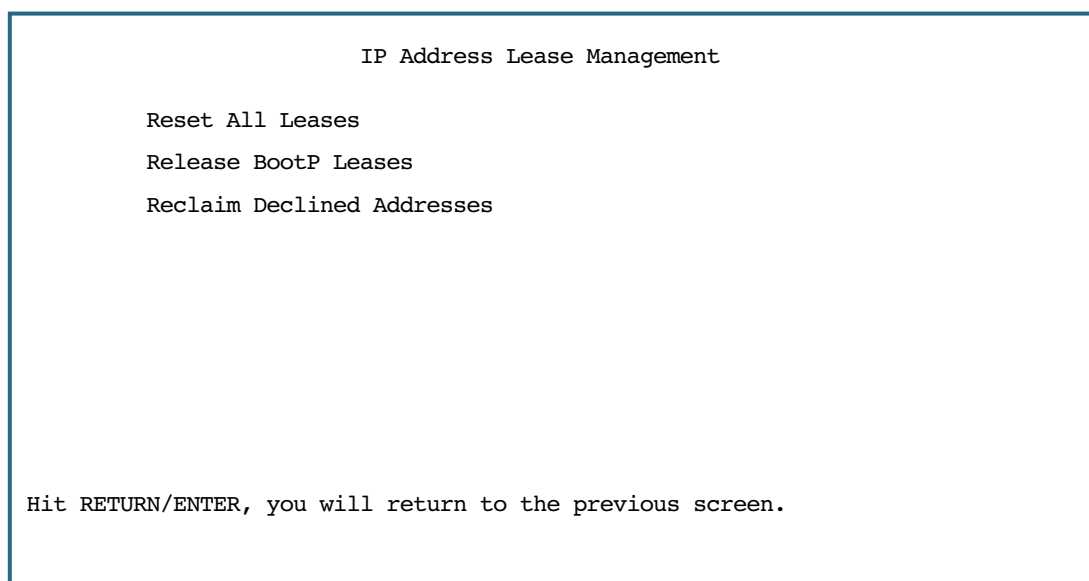
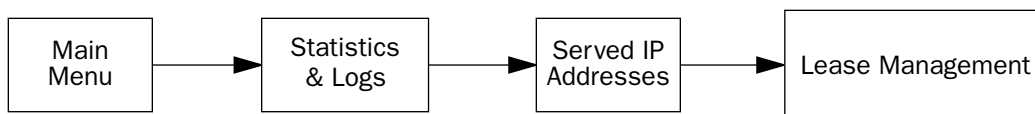
- To serve DHCP clients with the NetBIOS scope, select **Serve NetBIOS Scope** and toggle it to **Yes**.
Select **NetBIOS Scope** and enter the scope.
- To serve DHCP clients with the IP address of a NetBIOS name server, select **Serve NetBIOS Name Server** and toggle it to **Yes**.

Select **NetBIOS Name Server IP Addr** and enter the IP address for the NetBIOS name server.

You are now finished setting up DHCP NetBIOS Options. To return to the IP Address Serving screen, press Escape.

- To enable BootP's address serving capability, select **Serve BOOTP Clients** and toggle to **Yes**.

Note: Addresses assigned through BootP are permanently allocated from the IP Address Serving pool until you release them. To release these addresses, navigate back to the Main Menu, then Statistics & Logs, Served IP Addresses, and Lease Management.



Select **Release BootP Leases** and press Return.

- Back in IP Address Serving, the Serve Dynamic WAN Clients toggle

More Address Serving Options

The Netopia Firmware Version 8.4 includes a number of enhancements in the built-in DHCP IP address server. These enhancements include:

- The ability to exclude one or more IP addresses from the address serving pool so the addresses will not be served to clients.
- The ability to reserve a particular IP address for a client with a particular Ethernet MAC address.

6-24 *Firmware User Guide*

- The ability to view the host name associated with a client to which the gateway has leased an IP address.
- The ability for the gateway’s Ethernet IP address(es) to overlap the DHCP address serving pool(s).
- The ability to serve as a DHCP Relay Agent.

The Netopia Firmware Version 8.4 supports reserving an IP address only for a type 1 client identifier (i.e., an Ethernet hardware address). It does not support reserving an IP address for an arbitrary client identifier. (For more information on client identifiers, see RFC 2131, section 9.14.)

Configuring the IP Address Server options

To access the enhanced DHCP server functions, from the Main Menu navigate to **Statistics & Logs** and then **Served IP Addresses**.



The following example shows the Served IP Addresses screen after three clients have leased IP addresses. The first client did not provide a Host Name in its DHCP messages; the second and third clients did.

Served IP Addresses			
-IP Address-----	Type----	Expires--	Host Name/Client Identifier-----
-----SCROLL UP-----			
192.168.1.100			
192.168.1.101			
192.168.1.102			
192.168.1.103	DHCP	00:59	EN: 00-00-C5-70-00-04
192.168.1.104	DHCP	00:59	Bill's Pentium
192.168.1.105	DHCP	00:45	Steve's Power Mac
192.168.1.106			
192.168.1.107			
192.168.1.108			
192.168.1.109			
192.168.1.110			
192.168.1.111			
192.168.1.112			
192.168.1.113			
-----SCROLL DOWN-----			
Lease Management...			

The rightmost column displays the host name supplied by the client if one was provided; otherwise it displays the client identifier. (If a host name is displayed, the client identifier is still accessible in a Details pop-up menu. See below.)

Note: The server does not query the client for its host name. Macintosh computers running versions of MacOS prior to MacOS version 8.5 (OT 2.0.1, TCP/IP 2.0.1) do not supply a host name option in their DHCP messages, so no host name will appear in the Served IP Addresses list.

You can select the entries in the Served IP Addresses screen. Use the up and down arrow keys to move the selection to one of the entries in the list of served IP addresses.

Served IP Addresses			
-IP Address-----	Type----	Expires--	Host Name/Client Identifier-----
-----SCROLL UP-----			
192.168.1.100			
192.168.1.101			
192.168.1.102			
192.168.1.103			
192.168.1.104			
192.168.1.105			
192.168.1.106			
192.168.1.107			
192.168.1.108			Barr's XPi 120
192.168.1.109			
192.168.1.110			
192.168.1.111			
192.168.1.112			
192.168.1.113			
-----SCROLL DOWN-----			
Lease Management...			

Once you select an entry, pressing Return displays an action pop-up menu that lists operations that can be performed on that entry. Possible operations are **Details...**, **Exclude**, **Include**, **Release**, and **Reserve...**. The action popup is context-sensitive and lists only those operations that apply to the selected IP address in its current lease state.

- **Details...** is displayed if the entry is associated with both a host name and a client identifier.

Selecting **Details...** displays a pop-up menu that provides additional information associated with the IP address. The pop-up menu includes the IP address as well as the host name and client identifier supplied by the client to which the address is leased.

Served IP Addresses

-IP Address-----Type---Expires---Host Name/Client Identifier-----

-----SCROLL UP-----

192.168.1.100

192.168.1.101

-----+-----

-----+-----

IP Address is 192.168.1.108

Host Name is Barr's XPi 120

Client ID is EN: 00-00-c5-45-89-ef

-----OK-----

-----+-----

-----+-----

192.168.1.111 | Reserve... |

192.168.1.112 | -----+----- |

192.168.1.113

-----SCROLL DOWN-----

Lease Management...

- **Exclude** is displayed if the entry is not already excluded.

Selecting **Exclude** excludes the IP address from the address serving pool so the address will not be served to a client. If the IP address is currently leased to or reserved for a client, you will be presented with a warning dialog asking you to confirm the operation.

Served IP Addresses

-IP Address-----Type---Expires---Host Name/Client Identifier-----

-----SCROLL UP-----

192.168.1.100

192.168.1.101

192.1+-----+-----

192.1+-----+-----

192.1+-----+-----

192.1 | You are about to make changes that will affect an address

192.1 | that is currently in use. Are you sure you want to do this?

192.1 |

192.1 | CANCEL | OK

192.1 |

192.1+-----+-----

-----+-----

192.168.1.111 | Reserve... |

192.168.1.112 | -----+----- |

192.168.1.113

-----SCROLL DOWN-----

Lease Management...

- **Include** is displayed if the entry is either excluded or declined.

An IP address is marked declined when a client to whom the DHCP server offers the address declines the address. A client declines an address if it determines that a leased address is already in use by another device.

Selecting **Include** restores the selected IP address to the address serving pool so that the IP address is once again eligible to be served to a client.

- **Release** is displayed if the entry is currently offered, leased, or reserved.

Selecting **Release** puts the selected entry in the available state. You will be presented with a warning dialog asking you to confirm the operation since the IP address is in use. There is no mechanism to notify the client to whom the address is leased that the lease has been terminated. Thus, the client will continue to use the address until the next time it attempts to renew its lease. In the interim, the server may lease the same IP address to a different client, thereby creating an address conflict. For this reason, releasing an address that is actively being used by a client is generally not recommended.

- **Reserve...** is displayed if the entry is available, declined, excluded, leased, offered, or reserved.

Reserving an IP address for a client with a particular Ethernet MAC address guarantees that a client with the specified MAC address will be offered or leased the specified IP address. Moreover, it prevents the specified IP address from being offered or leased to any other client.

Selecting **Reserve...** displays a pop-up dialog box that displays the IP address and editable item in which you can enter an Ethernet MAC address. The pop-up dialog box includes **OK** and **CANCEL** buttons for confirming or cancelling the operation. If the IP address is currently offered or leased to, or reserved for, a client, you will be presented with a warning dialog asking you to confirm the operation. Reserving an IP address guarantees that the IP address will only be leased.

Served IP Addresses			
-IP Address-----	Type----	Expires--	Host Name/Client Identifier-----
-----SCROLL UP-----			
192.168.1.100			
192.168.1.101			
192.168.1.102			
192.168.1.103			
192.168.1.104			
192.168.1.105			
192.168.1.106			
192.168.1.107			
192.168.1.108			
192.168.1.109			
192.168.1.110			
192.168.1.111			
192.168.1.112			
192.168.1.113			
-----SCROLL DOWN-----			

IP Address is 192.168.1.108
 MAC Address: 00-00-c5-45-89-ef

CANCEL OK

Lease Management...

The gateway's Ethernet IP address(es) will be automatically excluded from the address serving pool(s) on startup. Entries in the served IP address list corresponding to the gateway's Ethernet IP address(es) that have been automatically excluded on startup are not selectable.

```

                                Served IP Addresses
-----IP Address-----Type----Expires--Host Name/Client Identifier-----
-----SCROLL UP-----
192.168.1.1      Excluded for the gateway's IP address
192.168.1.2      Excluded
192.168.1.3      DHCP      00:24      Barr's XPi 120
192.168.1.4
192.168.1.5
192.168.1.6
192.168.1.7
192.168.1.8
192.168.1.9
192.168.1.10
192.168.1.11
192.168.1.12
192.168.1.13
192.168.1.14
-----SCROLL DOWN-----
Lease Management...

Hit RETURN/ENTER for available operations.
```

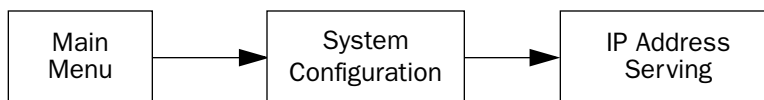
DHCP Relay Agent

The Netopia Firmware Version 8.4 offers DHCP Relay Agent functionality, as defined in RFC1542. A DHCP relay agent is a computer system or a gateway that is configured to forward DHCP requests from clients on the LAN to a remote DHCP server, and to pass the replies back to the requesting client systems.

When a DHCP client starts up, it has no IP address, nor does it know the IP address of a DHCP server. Therefore, it uses an IP broadcast to communicate with one or more DHCP servers. These broadcasts are normally limited to the network segment on which the client is located, and do not pass through gateways such as the Netopia Router. If the Netopia Router is configured to act as a DHCP server, it will assign the client an address from an address pool configured locally in the Netopia Router and respond to the client's request itself.

However, if the Netopia Router is configured to act as a DHCP relay agent, it does not satisfy the DHCP request itself, but instead forwards the request to one or more remote DHCP servers. These servers process the request, assign an address from an address pool configured on the remote server, and forward the response back to the Netopia Router for delivery back to the client. The agent then sends the response to the client on behalf of the DHCP server. This process is transparent to the client, which doesn't know that it is communicating through an intermediary rather than directly to a local server. Using DHCP relay, it is possible to centralize the configuration information for the host computers at many remote sites at a single location, easing the burden of administering configuration management for remote sites.

To configure the Netopia Router to act as a DHCP relay agent, from the Main Menu navigate to the System Configuration menu.



Select **IP Address Serving** and press Return. The IP Address Serving screen appears.

IP Address Serving	
IP Address Serving Mode...	<div style="border: 1px dashed black; padding: 2px;"> Disabled DHCP Server DHCP Relay Agent </div>
Number of Client IP Addresses:	
1st Client Address:	
Client Default Gateway...	192.168.1.1
Serve DHCP Clients:	Yes
DHCP NetBIOS Options...	
Serve BOOTP Clients:	Yes

Select **IP Address Serving Mode**. The pop-up menu offers the choices of **Disabled**, **DHCP Server** (the default), and **DHCP Relay Agent**.

If you select DHCP Relay Agent and press Return, the screen changes as shown below.

IP Address Serving

IP Address Serving Mode...	DHCP Relay Agent
Relay Server #1:	10.1.1.1
Relay Server #2:	20.1.1.1
Relay Server #3:	30.1.1.1

Configure Address Serving (DHCP, BOOTP, etc.) here.

Now you can enter the IP address(es) of your remote DHCP server(s), such as might be located in your company’s corporate headquarters. Each time you enter an IP address and press Return, an additional field appears. You can enter up to four DHCP server addresses.

In the example above, DHCP requests from clients on the LAN will be relayed to the DHCP servers at IP addresses 10.1.1.1, 20.1.1.1, and 30.1.1.1.

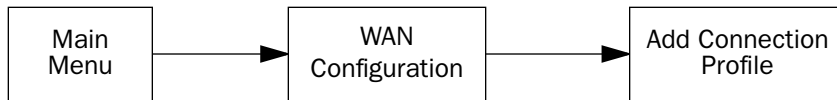
Note: The remote DHCP server(s) to which the Netopia Router is relaying DHCP requests must be capable of servicing relayed requests. Not all DHCP servers support this feature. For example, the DHCP server in the Netopia Router does *not*.

The DHCP server(s) to which the Netopia Router is relaying DHCP requests must be configured with one or more address pools that are within the Netopia Router’s primary Ethernet LAN subnet. (There is no mechanism for DHCP clients to receive an address on a secondary subnet via a relayed DHCP request.)

Connection Profiles

Since you will probably only have a single connection to your ISP over the DSL link, you may not need to create multiple connection profiles. Additional profiles may be useful for creating VPNs.

Connection Profiles define the line and networking protocols necessary for the gateway to make a remote connection. A connection profile is like an address book entry describing how the gateway is to get to a remote site, or how to recognize and authenticate a remote user connecting to the gateway. To create a new Connection Profile, you navigate to the WAN Configuration screen from the Main Menu, and select **Add Connection Profile**.



The Add Connection Profile screen appears.

Add Connection Profile	
Profile Name:	Profile 1
Profile Enabled:	Yes
Data Link Encapsulation...	PPP
Data Link Options...	
IP Profile Parameters...	
COMMIT	CANCEL
Configure a new Conn. Profile. Finished? COMMIT or CANCEL to exit.	

On a Router you can add up to 15 more connection profiles, for a total of 16, although only one can be used at a time, unless you are using VPNs.

1. Select **Profile Name** and enter a name for this connection profile. It can be any name you wish. For example: the name of your ISP.
2. Toggle the **Profile Enabled** value to **Yes** or **No**. The default is Yes.
3. Select **IP Profile Parameters** and press Return. The IP Profile Parameters screen appears.

IP Profile Parameters

Address Translation Enabled:

Yes

IP Addressing...

Numbered

NAT Map List...

Easy-PAT List

NAT Server List...

Easy-Servers

Local WAN IP Address:

0.0.0.0

Local WAN IP Mask:

0.0.0.0

Remote IP Address:

0.0.0.0

Remote IP Mask:

0.0.0.0

Filter Set...

Remove Filter Set

RIP Profile Options...

Configure IP requirements for a remote network connection here.

4. Toggle or enter any IP parameters you require and return to the Add Connection Profile screen by pressing Escape. For more information on NAT, see [“Multiple Network Address Translation,” beginning on page 3-1.](#)
- The Local WAN IP Address is displayed for numbered or NAT profiles. The Local WAN IP Mask is displayed for numbered profiles. The Remote IP Address and Remote IP Mask are displayed for unnumbered profiles.
5. Select **ADD PROFILE NOW** and press Return. Your new connection profile will be added.
- If you want to view the connection profiles in your gateway, return to the WAN Configuration screen, and select **Display/Change Connection Profile**. The list of connection profiles is displayed in a scrolling pop-up screen.

WAN Configuration

+--Profile Name-----IP Address-----+

Easy Setup Profile

127.0.0.2

Profile 1

0.0.0.0

on:

Yes

Up/Down Arrow Keys to select, ESC to dismiss, Return/Enter to Edit.

Multicast Forwarding

Multicast is a method for transmitting large amounts of information to many, but not all, hosts over an Internet. One common use is to distribute real time audio and video to the set of hosts which have joined a distributed conference.

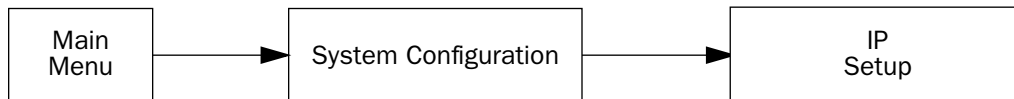
Multicast is similar to radio or TV broadcasts in the sense that only those who have tuned in to a particular frequency receive the information. You see and hear the channel you are interested in, but not the others.

Since a gateway should not be used as a passive forwarding device, Netopia gateways use a protocol for forwarding multicasting. This protocol is Internet Group Management Protocol (IGMP). Two versions of IGMP are available, V1 and V2. Netopia gateways can use either one, however, Multicast Forwarding will only work if your service provider supports it. Check with your service provider.

You configure Multicast Forwarding in two Telnet menu screens:

- First, you enable Multicast Forwarding in the **IP Setup** screen in the **System Configuration** menu,
- Then you associate it with a Connection Profile in the **IP Profile Parameters** screen in the **Add/Display/Change Connection Profile** menus.

Navigate to the **IP Setup** screen.



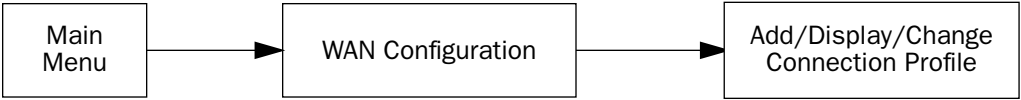
By default, Multicast Forwarding is tuned off (None). You enable the gateway to transmit multicast data by selecting **Tx.** from the pull-down menu.

IP Setup

Ethernet IP Address:	192.168.1.1
Ethernet Subnet Mask:	255.255.255.0
Define Additional Subnets...	
Default IP Gateway:	0.0.0.0
Backup IP Gateway:	0.0.0.0
Primary Domain Name Server:	0.0.0.0
Secondary Domain Name Server:	0.0.0.0
Domain Name:	
Receive RIP...	Both
Transmit RIP...	+-----+
Multicast Forwarding...	+-----+
IGMP Version...	None
	Tx.
	+-----+
Static Routes...	IP Address Serving...

If you enable Multicast Forwarding, you will see a new option **IGMP Version**. This lets you choose V1 or V2. If you know you will be communicating with other hosts that are limited to V1, select V1; otherwise, allow the default V2.

Navigate to the **IP Profile Parameters** screen.



IP Profile Parameters

Address Translation Enabled:	Yes
IP Addressing...	Numbered
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
Local WAN IP Address:	0.0.0.0
Local WAN IP Mask:	0.0.0.0
Remote IP Address:	0.0.0.0
Remote IP Mask:	0.0.0.0
Filter Set...	+-----+
Remove Filter Set	+-----+
	None
	Rx.
	+-----+
Multicast Forwarding...	
RIP Profile Options...	

Typically, you will have a Connection Profile that you created in Easy Setup. You may have more. Select the Connection Profile that you want to use from the **Display/Change Connection Profile** menu, and then select **IP Profile Parameters**.

By default, Multicast Forwarding is turned off (None) on Connection Profiles until you enable a specific Connection Profile to receive multicast data. You enable it by selecting **Rx.** from the pull-down menu.

Chapter 7

Line Backup

Netopia Firmware Version 8.4 offers line backup functionality in the event of a line failure on the primary WAN link:

- to an internal V.92 modem (supported models) or
- to a backup default gateway.

This chapter covers the following topics:

- [“Configuring Backup” on page 7-1](#)
- [“Connection Profiles” on page 7-2](#)
- [“WAN Configuration” on page 7-8](#)
- [“Using Scheduled Connections with Backup” on page 7-12](#)
- [“Backup Default Gateway” on page 7-14](#)
- [“Backup Management/Statistics” on page 7-17](#)
- [“QuickView” on page 7-18](#)

The purpose of line backup is to provide a recovery mechanism in the event that the primary connection fails. A failure can be either line loss, for example by central site switch failure or physical cable breakage, or loss of end-to-end connectivity. Detection of one of these failures causes the router to switch from using the primary DSL WAN connection to using a built-in V.92 modem. Alternatively, you can choose backup to an alternate gateway on the Ethernet LAN. In the event of a loss of primary connectivity you have the option of switching back to the primary port automatically once it has recovered its connection.

Configuring Backup

The following menus support backup configuration:

- the **Add Connection Profile** menus under the **WAN Configuration** menus

Here you choose **Encapsulation Type** = **PPP**, fill out the correct **IP Profile Parameters** information, select **Backup** as the **Interface Group**, and fill out the **Telco Options**. See [“Connection Profiles” on page 7-2](#).

- the **MODEM (Wan Module 2) Setup** menu under the **WAN Configuration, WAN (Wide Area Network) Setup** menus

Here you configure the **Internal Modem Setup** that governs a number of general behavior settings for the internal V.92 modem. See [“WAN Configuration” on page 7-8](#).

- the **Backup Configuration** menu under **WAN Configuration, Advanced Connection Options**

Here you can select **Backup is** = **Automatic**, and **Recovery** is **Automatic**. See [“Backup Configuration screen” on page 7-10](#).

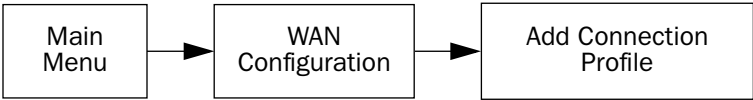
- the **Backup IP Gateway** menu item in the **IP Setup** screen under the **System Configuration** menu
- Here you enter a Backup Gateway IP address. See [“IP Setup” on page 7-7](#). Alternatively, you can choose a different backup gateway device; see [“Backup Default Gateway” on page 7-14](#).

Detailed descriptions follow.

Connection Profiles

The dial backup feature allows you to configure a complete Connection Profile for the modem backup, just as you do for your primary WAN connection. In this way profiles are associated with a particular interface. It should have switched characteristics for modem backup.

Navigate to the **Add Connection Profile** screen.



Add Connection Profile

Profile Name:

Profile 1

Profile Enabled:

Yes

Encapsulation Type...

RFC1483

RFC1483 Mode...

Bridged 1483

IP Profile Parameters...

COMMIT

CANCEL

Return accepts * ESC cancels * Left/Right moves insertion point * Del deletes.

Configure a new Conn. Profile. Finished? COMMIT or CANCEL to exit.

If you used Easy Setup to configure your DSL connection, you have already created one Connection Profile. For the backup modem, you create a second Connection Profile, and associate it with the backup modem interface.

- Profile Name:** Give the profile a descriptive name, for example “Modem Backup”.
- Profile Enabled:** Ordinarily this is toggled to **Yes**. You can toggle it to **No**, if you want to disable it later.
- Encapsulation Type:** From the pull-down menu select the encapsulation type. Usually, for modem dial-up connections, this will be **PPP**, but you can also select **ATMP**, **PPTP**, or **IPsec** for VPN connections. These are the options needed for dial-up.

Add Connection Profile	
Profile Name:	Profile 1
Profile Enabled:	+-----+
Encapsulation Type...	+-----+
Encapsulation Options...	PPP
IP Profile Parameters...	RFC1483
	ATMP
	PPTP
	IPsec
	L2TP
	+-----+
COMMIT	CANCEL

Assuming you selected PPP, new fields appear.

Add Connection Profile	
Profile Name:	Modem Backup
Profile Enabled:	Yes
Encapsulation Type...	PPP
Encapsulation Options...	
IP Profile Parameters...	
Interface Group...	+-----+
Telco Options...	+-----+
	Primary
	Backup
	+-----+
COMMIT	CANCEL

Underlying Encapsulation and **PPP Mode** do not usually need to be changed for a PPP connection.

- From the **Interface Group** pull-down menu, select **Backup**.
- Select **Encapsulation Options**.

7-4 *Firmware User Guide*

The Datalink (PPP/MP) Options screen appears.

Datalink (PPP/MP) Options

Data Compression...

+-----+rd LZS

Send Authentication...

+-----+

None
PAP
CHAP

+-----+

Send User Name:

Send Password:

Receive User Name:

Receive Password:

Dial on Demand:

Yes

PAP-- Password protection is used. Passwords are exchanged in clear text.

- **Data Compression** should remain set to Standard LZS.
- Usually, you use **PAP** Authentication, with a dial-up connection, but you can also use **CHAP**, or **None**.

For PAP Authentication, you enter your **User Name** and **Password**, and a **User Name** and **Password** for authorization of dial-in connections (if so configured). For CHAP Authentication, you enter a **Host Name** and **Secret**.

Unless otherwise instructed, you can leave the other defaults unchanged.

Press Escape.

Add Connection Profile

Profile Name:

Modem Backup

Profile Enabled:

Yes

Encapsulation Type...

PPP

Encapsulation Options...

IP Profile Parameters...

Interface Group...

Backup

Telco Options...

COMMIT

CANCEL

Configure a new Conn. Profile. Finished? COMMIT or CANCEL to exit.

- Select **IP Profile Parameters**. The IP Profile Parameters screen appears.

IP Profile Parameters

Address Translation Enabled:	Yes
IP Addressing...	Unnumbered
NAT Map List...	Easy-PAT List
NAT Server List...	Easy-Servers
NAT Options...	
Stateful Inspection Enabled:	No
Local WAN IP Address:	0.0.0.0
Remote IP Address:	0.0.0.0
Remote IP Mask:	0.0.0.0
Filter Set...	
Remove Filter Set	
RIP Profile Options...	
Toggle to Yes if this is a single IP address ISP account.	
Configure IP requirements for a remote network connection here.	

- Unless otherwise instructed, accept the defaults, except the following:
 - Set **Remote IP Address** to 127.0.0.2.
 - Set **Remote IP Mask** to 255.255.255.0.

These allow your ISP to supply your IP address and subnet mask when you connect via dial-up.

Press Escape to return to the Add Connection Profile screen.

- When you chose Backup for the Interface Group, **Telco Options** became visible. Select **Telco Options**. The Telco Options screen allows you to set the parameters for the modem connection.

Telco Options	
Dial...	Dial In/Out
Dialing Prefix:	
Number to Dial:	
Alternate Site to Dial:	
Dial on Demand:	Yes
Idle Timeout (seconds):	300
Callback:	No
CompuServe Login Enabled:	No

- From the **Dial** pop-up menu, you can choose whether to Dial Out Only, Dial In Only, or Dial In/Out (default).
- **Dialing Prefix:** If you are connected to a Centrex or PBX phone system that requires you to dial a prefix number (such as “9” for an outside line), enter it here.
- You can add the **Number to Dial** and an **Alternate Site to Dial**, if available.
- You can toggle **Dial on Demand** to Yes or No. This allows the router to determine whether or not to dial the backup number when there is traffic that needs to be transmitted or received.
- You can set the **Idle Timeout (seconds)** to tear down the connection after some specified period of inactivity.
- You can also toggle **Callback** to No or Yes. In most cases, since this is a backup connection, you can leave this set to the default No.
- In some cases, your service provider or corporate office may use the CompuServe Login protocol. If so, toggle **CompuServe Login Enabled** to **Yes**. Otherwise, leave the default **No**.

When enabled, CompuServe Login requires that you enter a **CompuServe Host Name**, a **CompuServe User Name**, and a **CompuServe Password**. These options become visible only if you enable CompuServe Login.

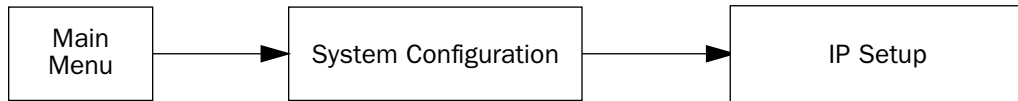
Press Escape. You are returned to the Add Connection Profile screen.

Select **COMMIT**, and press Return. Your backup Connection Profile will be created and enabled.

IP Setup

Here, you set the IP address of the alternate gateway.

Navigate to the **IP Setup** screen under the **System Configuration** menu.



IP Setup

Ethernet IP Address:	192.168.1.1
Ethernet Subnet Mask:	255.255.255.0
Define Additional Subnets...	
Default IP Gateway:	0.0.0.0
Backup IP Gateway:	0.0.0.0
Primary Domain Name Server:	0.0.0.0
Secondary Domain Name Server:	0.0.0.0
Domain Name:	
Rip Options...	
Multicast Forwarding...	None
Static Routes...	IP Address Serving...

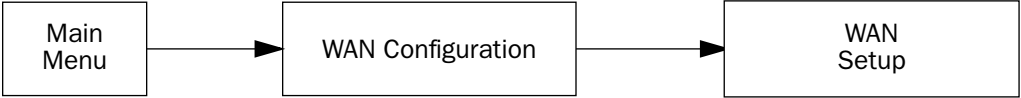
Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
Set up the basic IP attributes of your Netopia in this screen.

- Set **Backup IP Gateway** to 127.0.0.2.
- Set **Secondary Domain Name Server** to the IP Address DNS of your dial-up ISP.

For information about the Backup Default Gateway option, see [“Backup Default Gateway” on page 7-14](#).

WAN Configuration

To configure the modem characteristics, from the Main Menu select **WAN Configuration** and then **WAN Setup**.



WAN Configuration

WAN (Wide Area Network) Setup...
ATM Circuits Configuration...

Display/Change Connection Profile...
Add Connection Profile...
Delete Connection Profile...

WAN Default Profile...
ATMP/PPTP Default Profile...
IKE Phase 1 Configuration...

Advanced Connection Options...

Return/Enter to create a new Connection Profile.
From here you will configure yours and the remote sites' WAN information.

The **Choose Interface to Configure** screen appears. These settings govern the general modem behavior.

Choose Interface to Configure

ADSL Setup...
MODEM (Wan Module 2) Setup...

Choose the interface to configure for backup, **MODEM (Wan Module 2) Setup**.

The Internal Modem Setup screen appears.

Internal Modem Setup

Modem Dialing Prefix:	ATDT
PBX Dialing Prefix:	
Line Directory Number:	
Speaker On...	Until Carrier
Speaker Volume...	2-Medium
Answer Incoming calls...	Always
Country...	United States

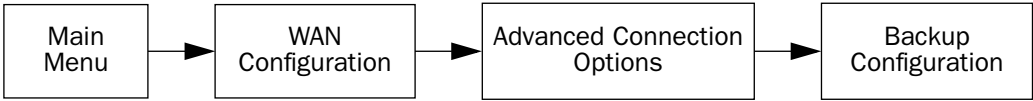
Enter the dialing prefix to be sent to all modems.

- **Modem Dialing Prefix:** ATDT is the standard Hayes-compatible code for alerting the modem itself. You probably don't need to change this, unless you have a good reason and are familiar with the Hayes modem command set.
- **PBX Dialing Prefix:** If you are connected to a Centrex or PBX phone system that requires you to dial a prefix number (such as "9" for an outside line), enter it here.
- **Line Directory Number:** Enter the telephone number for the line you are connected to.
- **Speaker On:** You can set how you want to hear dialing and connection tones generated by the modem, or you can turn them off, from the pull-down menu. Options are: Never, Until Carrier, During Answer, Always.
- **Speaker Volume:** You can set how loud the modem tones will be from the pull-down menu: 1-Softest, 2-Medium, 3-Loudest.
- **Answer Incoming calls:** You can determine whether or not the modem will respond to incoming calls on this line, from the pull-down menu: Always or Never.
- **Country:** Select your country from the pull-down menu.

When you are finished, press Escape.

Backup Configuration screen

Navigate to the Backup Configuration screen.



This screen is used to configure the conditions under which backup will occur, if it will recover, and how the modem is configured.

For the internal V.92 modem, the Backup Configuration screen appears as follows, when all options are enabled (default screen shows fewer menu items until some are enabled):

Backup Configuration

Backup Parameters

Backup is... Automatic

Requires Failure of (minutes): 1

Ping Host Name or IP Address:

Recovery to ADSL... Automatic

Requires Recovery of (minutes): 1

Clear Backup Call only if idle: No

Data Link Encapsulation is Async PPP

Enter Information supplied to you by your telephone company.

- Select **Backup is** and from the pop-up menu, select Automatic (default), Manual, or Disabled. You enable line backup by selecting either Manual or Automatic. For fail-over purposes, choose Automatic.
- Select **Requires Failure of (minutes)** and enter the number of minutes that the system should wait before it assumes that a connection failure has occurred. After that period, the system would switch to backup mode and connect via the modem.

Note: Backup and Recovery have resolutions of five seconds. This is how often the router evaluates the state of the connections and makes decisions.

- Select **Ping Host Name or IP Address** and enter an IP address or resolvable DNS name that the router will ping. This is an optional item that is particularly useful for testing if the remote end of a VPN connection

has gone down. Should this address become unreachable the router will treat this as a loss of connectivity and begin the backup timer. This loss is a Layer 2 loss.

Note: For best results, enter an IP address and not a host name. If a host name is used it may not be resolvable, and may keep the interface down.

Set the Ping Host Name or IP Address to the router's Default Gateway, or other reliable IP address elsewhere on the backbone – for example, a DNS server. This will ensure that the router will initiate backup connection on loss of Layer 3.

Note: If you want the router to initiate the backup connection on loss of Layer 1 or 2 only (Physical or Data link Layer), leave Ping Host Name or IP Address blank. Do *not* use 0.0.0.0 in this field. Hit the space bar or Delete key to CLEAR the field totally. Leaving 0.0.0.0 in this field tells the router to ping an address that does not exist.

- Select **Recovery to ADSL** and press Return. Choose either Manual or Automatic to determine how the system will return to the primary WAN link when it becomes available again. If you choose Automatic, the next two menu items become visible.

Note: Automatic recovery only works upon loss of primary WAN connectivity.

- If you chose Automatic Recovery, select **Requires Recovery of (minutes)** and enter the number of minutes that the system should wait before it assumes that a connection has been re-established. This allows you to be sure that the primary WAN connection is well re-established before the router switches back to it from the backup mode. If the router's primary connection fails at layer 1, the **Requires Recovery of (minutes)** parameter determines the amount of time the primary layer 1 connection must be up (recovered) before the router will tear down the backup connection and revert to the primary interface.
- Select **Clear Backup Call only if idle**. The default Yes will prevent the backup call from being torn down if there is activity on the backup connection when the primary connection comes back up. You can toggle this to No if you wish.

The **Clear Backup Call only if Idle** timer is a separate timer from the **Requires Recovery of (minutes)** timer. The router will first reach the Requires Recovery of (minutes) counter and count down to zero. Then the router will consult the Clear Backup Call only if Idle timer to learn if the backup connection has been idle for the specified seconds. If the connection has been idle for the specified seconds, then the teardown process of the backup connection will begin.

- **Requires idle time of (seconds)** specifies how long the device should wait before permitting the call to be torn down after a period of inactivity.
- **Data Link Encapsulation** is set to Async PPP. This field is not editable.

When you are finished, press Escape.

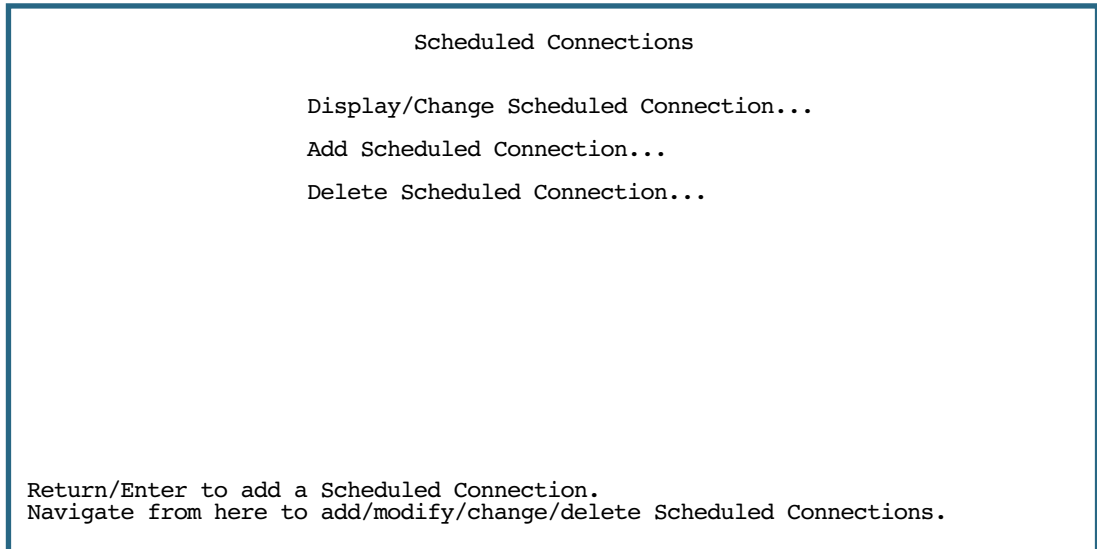
Using Scheduled Connections with Backup

The backup link is a PPP dial-up connection and only connects to the Internet service provider when traffic is initiated from the LAN. If you want to use the backup link to provide redundancy for services, such as a Web service that you provide to the outside world, you must force the connection to stay up. You do this by creating a scheduled connection entry that will be a permanent “forced up” connection for the backup modem. The backup modem will be activated upon primary WAN link failure and remain active until primary WAN link recovery.

To configure a Scheduled Connection, from the Main Menu select WAN Configuration and then Scheduled Connections.



The Scheduled Connections screen appears.



- Select **Add Scheduled Connection** and press Return. The Add Scheduled Connection screen appears.

Add Scheduled Connection

Scheduled Connection Enable:	On
How Often...	Weekly
Schedule Type...	Forced Up
Set Weekly Schedule...	
Use Connection Profile...	

ADD SCHEDULED CONNECTION CANCEL

Return/Enter accepts * Tab toggles * ESC cancels.
 Scheduled Connections dial remote Networks on a Weekly or Once-Only basis.

- Toggle **Scheduled Connection Enable** to **On**.
- From the **How Often** pop-up menu, select **Weekly** and press Return.
- From the **Schedule Type** pop-up menu, accept the default **Forced Up** and press Return.
- Select **Set Weekly Schedule**, and press Return. The Set Weekly Schedule screen appears.

Set Weekly Schedule

Monday:	Yes
Tuesday:	Yes
Wednesday:	Yes
Thursday:	Yes
Friday:	Yes
Saturday:	Yes
Sunday:	Yes

Scheduled Window Start Time:	11:27
AM or PM:	AM

Scheduled Window Duration Per Day: 24:00

Return/Enter accepts * Tab toggles * ESC cancels.

- Toggle all the days of the week to **Yes**, and set the **Scheduled Window Duration Per Day** to **24:00**. This guarantees a 24X7 connection. Press Escape to return to the Add Scheduled Connection screen.

7-14 Firmware User Guide

- Select **Use Connection Profile**, and press Return. A screen displays all of your Connection Profiles. Select the one you want to apply this scheduled connection to and press Return. Your selection becomes effective.

Now, if your primary WAN link fails, the backup link will become active and remain active until the primary link recovers.

Backup Default Gateway

If your Netopia equipment does not have an internal modem, or if you do not want to use the internal modem for backup, the Netopia Firmware Version 8.4 offers backup functionality to an alternate gateway typically connected to a LAN port.

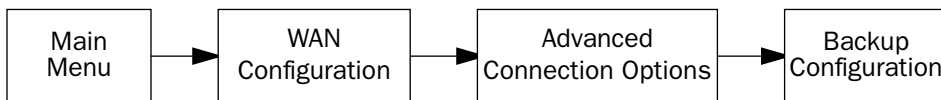
A typical application would be to have a LAN connection from your 3300-Series gateway to another gateway that has, for example, an ISDN or analog modem connection to the Internet, and designating the second gateway as the backup gateway. Should the primary WAN connection fail, traffic would be automatically redirected through your alternate gateway device to maintain Internet connectivity.

Two menus control the backup gateway feature:

- the **Backup Configuration** screen in the **WAN Configuration** menu
Here, you enable the backup feature and set some parameters.
- the **IP Setup** screen in the **System Configuration** menu
Here, you set the IP address of the alternate gateway device.

Backup Configuration screen

To enable the backup feature, from the Main Menu select **WAN Configuration**, **Advanced Connection Options**, and then **Backup Configuration**.



The Backup Configuration screen appears.

Backup Configuration	
Backup Parameters	
Backup is...	Disabled
Requires Failure of (minutes):	Manual
Ping Host Name or IP Address:	Automatic
Recovery to ADSL...	Automatic
Requires Recovery of (minutes):	1
Auto-Recovery on loss of Layer 2:	No

Automatically switches to Backup Port on loss of Layer 1 or 2.

This screen is used to configure the conditions under which backup will occur, if it will recover, and how the alternate gateway is configured.

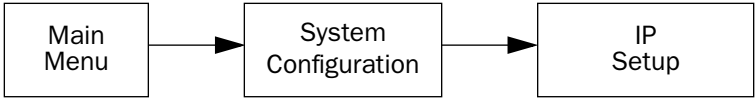
- Select **Backup is** and press Return. A pop-up menu allows you to select Disabled, Manual, or Automatic. You enable backup by selecting either Manual or Automatic. If you enable backup, the subsequent menu items become visible.
- Select **Requires Data Link Failure of (minutes)**. Enter the number of minutes you want the system to wait before the backup port becomes enabled in the event of primary line failure. This allows you to be sure the WAN connection is not merely briefly interrupted before the gateway switches to backup mode.
- Select **Ping Host Name or IP Address** and enter an IP address or resolvable DNS name that the gateway will ping. This is an optional item that is particularly useful for testing if the remote end of a VPN connection has gone down. Should this address become unreachable the gateway will treat this as a loss of connectivity and begin the backup timer. This loss is a Layer 2 loss.

Note: For best results, enter an IP address and not a host name. If a host name is used it may not be resolvable, and may keep the interface down.

- Select **Recovery to "WAN_name"** (where *WAN_name* is the type of WAN connection you have, such as ADSL) and press Return. Choose either Manual or Automatic to determine how the system will return to the WAN link when it becomes available again. If you choose Automatic, the next two menu items become visible.
 - If you chose Automatic Recovery, select **Requires Recovery of**. Enter the number of minutes you want the system to wait before attempting to switch back to the WAN connection. This allows you to be sure that the WAN connection is well re-established before the gateway switches back to it from the backup mode.
- Press Escape twice to return to the Main Menu.

IP Setup screen

To configure the backup gateway, from the Main Menu select **System Configuration** then **IP Setup**.



The IP Setup screen appears.

The IP Setup screen permits entry of a backup IP gateway address. This field is always visible, even if the **Default IP Gateway** field is not filled out, as in the case of a DHCP-acquired IP address and default gateway on the WAN interface.

IP Setup

Ethernet IP Address:	192.168.1.1
Ethernet Subnet Mask:	255.255.255.0
Define Additional Subnets...	
Default IP Gateway:	0.0.0.0
Backup IP Gateway:	0.0.0.0
Primary Domain Name Server:	0.0.0.0
Secondary Domain Name Server:	0.0.0.0
Domain Name:	
Receive RIP...	Both
Transmit RIP...	Off

Static Routes... IP Address Serving...

Network Address Translation (NAT)...

Enter an IP address in decimal and dot form (xxx.xxx.xxx.xxx).
Set up the basic IP attributes of your Netopia in this screen.

For more information on IP Setup see the [“IP Setup” on page 6-2](#).

Note: Backup and Recovery have resolutions of five seconds. This is how often the gateway evaluates the state of the connections and makes decisions.

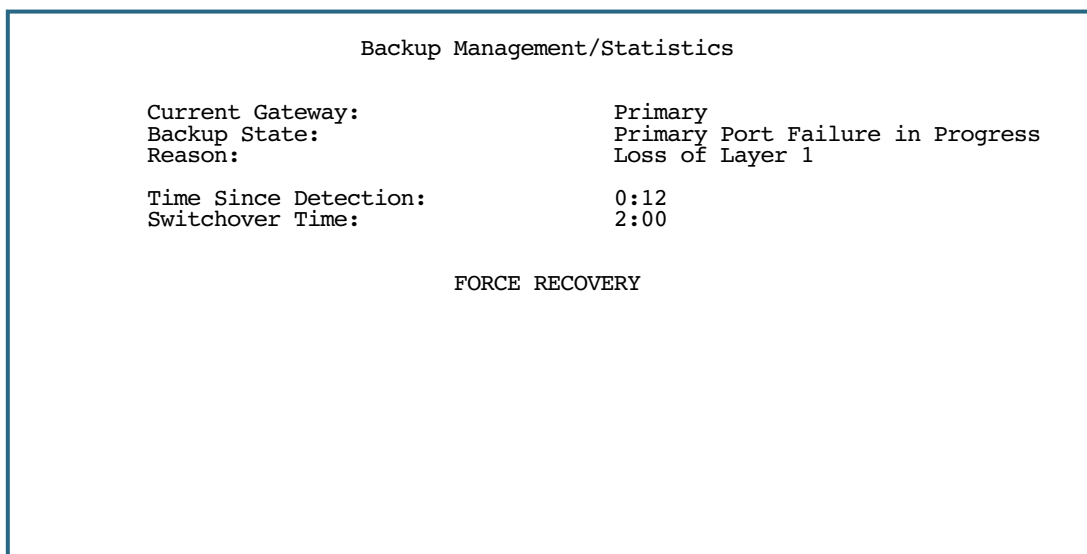
Backup Management/Statistics

If backup is enabled, the Statistics & Logs menu offers a Backup Management/Statistics option.

To view Backup Management/Statistics, from the Main Menu select **Statistics & Logs** then **Backup Management/Statistics** and press Return.



The Backup Management/Statistics screen appears.



- **Current Gateway** is a display-only field that shows which port is currently in operation.
- **Backup State** is a display-only field that shows the current state of Backup or Recovery.
- **Reason** becomes visible when a failure of or recovery to the Primary interface is in progress.

During backup, the following reasons may appear:

Loss of Layer 1	Indicates a loss of sync on the Primary link
Loss of Layer 2	Indicates connection profile cannot come up
Loss of Layer 2 (ping)	Indicates Backup Ping Address not responding
Loss of Layer 2 (Protocol Failure)	Indicates Primary link not responding to Protocol check (LCP Echo, LMI Status Request)

During recovery, the following reasons may appear:

Recovery of Layer 1	Indicates sync restored on the Primary link
Layer 2 Override	Indicates the backup occurred on layer 2, and 'Auto-Recovery on loss of Layer 2' was set to YES
Layer 2 Recovery	Indicates that backup was on Layer 2 and the interface is fully restored (including Backup Ping)

- **Time Since Detection** is a display-only field that is only visible if backup or recovery is in progress. It displays the elapsed time since detection of either WAN line failure or re-establishment of the connection.
- **Switchover Time** displays how high the *Time Since Detection* will count before the interface switches, either from Primary to Backup or from Backup to Primary.

This field is only visible if Backup or Recovery is set to **Automatic**.

When the current interface is Primary and a backup condition exists **Switchover Time** will display one of two values:

- If the last backup event was on layer 2 and **Auto-Recovery on loss of Layer 2** is set to **YES**, it will display the *Layer 2 Failure Timer* value.
- If this is the first backup event, or the last backup event was on layer 1, it will display the *Requires Failure of* value.

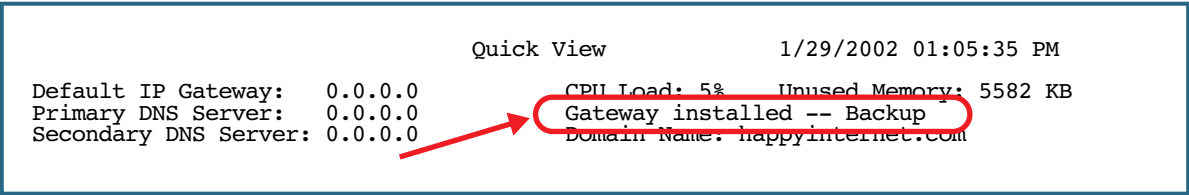
When the current interface is the Backup interface and a recovery condition exists, it will display the *Requires Recovery of* value.

The displayed value does not change. Rather it indicates how high the *Time Since Detection* must count before the switchover occurs.

- The **FORCE BACKUP/FORCE RECOVERY** option is a selectable option that, depending on the current state of backup, will force the switching of gateways. If you are currently in backup mode, the option will be **FORCE RECOVERY**. If you are currently in primary mode, the option will be **FORCE BACKUP**. Selecting either one and pressing Return will force the link to switch to the other mode.

QuickView

The QuickView screen now has an information element to indicate which gateway is in use.



Chapter 8

Monitoring Tools

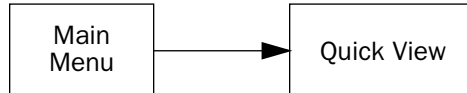
This chapter discusses the Router's device and network monitoring tools. These tools can provide statistical information, report on current network status, record events, and help in diagnosing and locating problems.

This section covers the following topics:

- [“Quick View Status Overview” on page 8-1](#)
- [“Statistics & Logs” on page 8-4](#)
- [“Event Histories” on page 8-4](#)
- [“IP Routing Table” on page 8-7](#)
- [“General Statistics” on page 8-7](#)
- [“System Information” on page 8-9](#)
- [“Simple Network Management Protocol \(SNMP\)” on page 8-10](#)

Quick View Status Overview

You can get a useful, overall status report from the Netopia Firmware Version 8.4 in the Quick View screen. To go to the Quick View screen, select **Quick View** in the Main Menu.



The Quick View screen has three status sections:

- General status
- Current DSL Status
- LED Status

General status

Quick View

10/11/2002 07:31:26 AM

Default IP Gateway: 0.0.0.0

CPU Load: 4%

Unused Memory: 6044 KB

Primary DNS Server: 0.0.0.0

Gateway installed -- Backup

Domain Name: netopia.com

Secondary DNS Server: 0.0.0.0

-----MAC Address-----IP Address-----Status-----

Ethernet LAN: 00-00-c5-ff-70-00 192.168.1.1 100Mbps Full Duplex

ATM ADSL WAN: 00-00-c5-ff-70-02 0.0.0.0

USB LAN: 00-00-c5-9a-09-a9 192.168.1.1 Down

Current WAN Connection Status

Profile Name-----Rate--%Use-Remote Address-----Est.-More Info-----

ISP 1536 10 IP 92.163.4.1 Lcl NAT 192.163.100.6

VPN QuickView

LED Status

-PWR---USB---DSL Link Activity--ETHERNET Activity Link--+-----LEDS-----

G - - - G G | '- ' = Off 'G' = Green

'R' = Red 'Y' = Yellow

Current Date: The current date; this can be set with the Date and Time utility (see [“Date and time” on page 2-29](#)).

Default IP Gateway: The gateway’s default gateway, which may be either manually configured or learned via DHCP. This is the value you assigned in the Default IP Gateway field. If you are using the gateway’s defaults (DHCP and NAT) this value will be 0.0.0.0. If you have assigned an IP address as your default gateway, it is shown here.

CPU Load: Percentage of the system’s resources being used by all current transmissions.

Unused Memory: The total remaining system memory available for use.

Primary DNS Server: If you are using the gateway’s defaults (DHCP and NAT) this value will be 0.0.0.0. If you have assigned an IP address as your primary default gateway, it is shown here.

Secondary DNS Server: If you are using the gateway’s defaults (DHCP and NAT) this value will be 0.0.0.0. If you have assigned an IP address as a secondary gateway, it is shown here.

Domain Name: The domain name you have assigned, typically the name of your ISP.

MAC Address: The Router’s hardware address, for those interfaces that support DHCP.

IP Address: The Router’s IP address, entered in the IP Setup screen.

Current status

The current status section is a table showing the current status of the DSL connection. For example:

Current WAN Connection Status					
Profile Name-----	Rate--	%Use-	Remote Address-----	Est.-	More Info-----
ISP	1536	10	IP 92.163.4.1	Lcl	NAT 192.163.100.6

Profile Name: Lists the name of the connection profile being used, if any.

Rate: Shows the line rate for this connection.

%Use: Indicates the average percent utilization of the maximum capacity of the channels in use for the connection.

Remote Address: Shows the IP address of the connected remote gateway.

Est: Indicates whether the connection was locally (“Lcl”) or remotely (“Rmt”) established.

More Info: Indicates the NAT address in use for this connection.

Status lights

This section shows the current real-time status of the Router’s status lights (LEDs). It is useful for remotely monitoring the gateway’s status. The Quick View screen’s arrangement of LEDs corresponds to the physical arrangement of LEDs on the gateway. These LEDs and the corresponding display in the Telnet menu screen will vary by model.

LED Status					
-PWR---	USB---	DSL Link Activity--	ETHERNET Activity Link--	+	-----LEDS-----
G	-	-	-	G	G
					'-'= Off 'G'= Green 'R'= Red 'Y'= Yellow

Each LED representation can report one of four states:

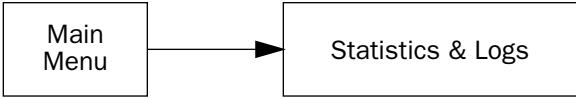
-: The LED is off.

R: The LED is red.

G: The LED is green.

Y: The LED is yellow.

Statistics & Logs



When you are troubleshooting your Router, the Statistics & Logs screens provide insight into the recent event activities of the gateway.

From the Main Menu go to Statistics & Logs and select one of the options described in the sections below.

Event Histories



The Netopia Firmware Version 8.4 records certain relevant occurrences in event histories. Event histories are useful for diagnosing problems because they list what happened before, during, and after a problem occurs. You can view two different event histories: one for the gateway’s system and one for the WAN.

The gateway’s event histories are structured to display the most recent events first, and to make it easy to distinguish error messages from informational messages. Error messages are prefixed with an asterisk. Both the WAN Event History and Device Event History retain records of the 128 most recent events.

In the Statistics & Logs screen, select **WAN Event History** or **Device Event History**.

WAN Event History

The WAN Event History screen lists a total of 128 events on the WAN. The most recent events appear at the top.

```

                                WAN Event History
                                Current Date -- 10/11/2003 03:02:23 PM
-Date-----Time-----Event-----
                                SCROLL UP
07/03/03 13:59:06   DSL: IP up, channel 1, gateway: 173.166.107.1
07/03/03 13:59:05   DSL: Channel 1 up
07/03/03 13:59:05 >>WAN: data link activated at 1040 Kbps
07/03/03 13:58:32 --Device restarted-----
07/03/03 12:46:39 --Device restarted-----
07/03/03 11:45:57 --Device restarted-----
07/02/03 17:58:15   DSL: IP up, channel 1, gateway: 173.166.107.1
07/02/03 17:58:10   DSL: Channel 1 up
07/02/03 17:58:10 >>WAN: data link activated at 1040 Kbps
07/02/03 17:57:05   DSL: IP down, channel 1
07/02/03 17:57:05   Link 1 down: No Synch
07/02/03 17:57:05 >>WAN: data link deactivated
07/02/03 17:48:02   DSL: IP up, channel 1, gateway: 173.166.107.1
07/02/03 17:48:01   DSL: Channel 1 up
                                SCROLL DOWN
Clear History...

Return/Enter on event item for details or SCROLL [UP/DOWN] item for scrolling.

```

Each entry in the list contains the following information:

Date: Date of the event.

Time: Time of the event.

Event: A brief description of the event.

Ch.: The channel involved in the event.

The first event in each call sequence is marked with double arrows (>>).

Failures are marked with an asterisk (*).

If the event history exceeds the size of the screen, you can scroll through it by using the SCROLL UP and SCROLL DOWN items.

To scroll up, select **SCROLL UP** at the top of the list and press Return. To scroll down, select **SCROLL DOWN** at the bottom of the list and press Return.

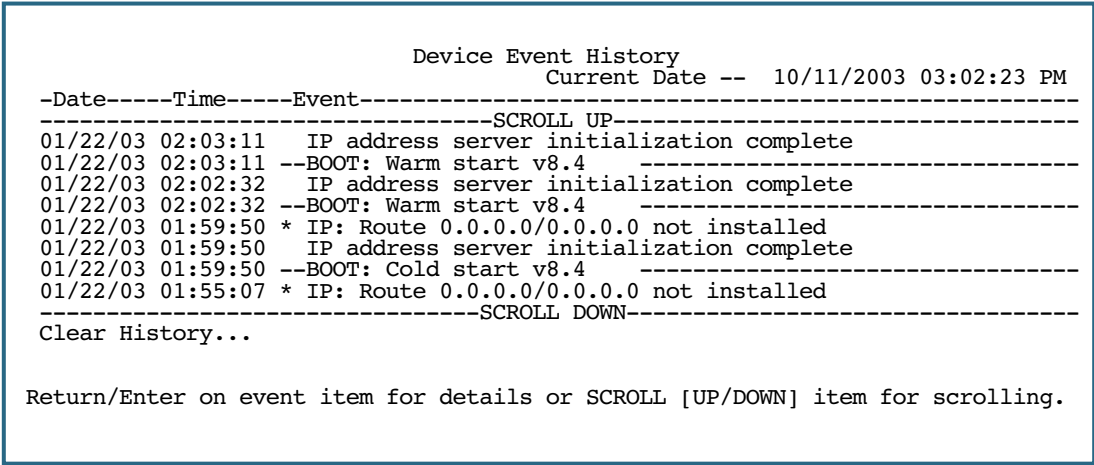
To get more information about any event listed in the WAN Event History, select the event and then press Return. A dialog box containing more information about the selected event will appear. Press Return or Escape to dismiss the dialog box.

To clear the event history, select **Clear History** at the bottom of the history screen and press Return.

Device Event History

The Device Event History screen lists a total of 128 port and system events, giving the time and date for each event, as well as a brief description. The most recent events appear at the top.

In the Statistics & Logs screen, select **Device Event History**. The Device Event History screen appears.



If the event history exceeds the size of the screen, you can scroll through it by using SCROLL UP and SCROLL DOWN.

To scroll up, select **SCROLL UP** at the top of the list and press Return. To scroll down, select **SCROLL DOWN** at the bottom of the list and press Return.

To obtain more information about any event listed in the Device Event History, select the event and then press Return. A dialog box containing more information about the selected event appears. Press Return or Escape to dismiss the dialog box.

To clear the Device Event History, select **Clear History** and press Return.

IP Routing Table



The IP routing table displays all of the IP routes currently known to the Router.

IP Routing Table					
Network Address	Subnet Mask	via Gateway	Port	Type	
-----SCROLL UP-----					
0.0.0.0	255.0.0.0	0.0.0.0	--	Other	
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	Local	
192.168.1.0	255.255.255.240	192.168.1.1	Ethernet	Local	
192.168.1.1	255.255.255.255	192.168.1.1	Ethernet	Local	
192.168.1.15	255.255.255.255	192.168.1.15	Ethernet	Bcast	
224.0.0.0	224.0.0.0	0.0.0.0	--	Other	
255.255.255.255	255.255.255.255	255.255.255.255	--	Bcast	
-----SCROLL DOWN-----					
UPDATE					

The routing table screen represents a snapshot of the routing table information at the time the screen is first invoked. To take a new snapshot, select **Update** at the bottom of the screen and press Return.

General Statistics



The General Statistics screen displays information about data traffic on the Router's data ports. This information is useful for monitoring and troubleshooting your LAN. Note that the counters roll over at their maximum field width, that is, they restart again at 0.

General Statistics						
Physical I/F	Rx Bytes	Tx Bytes	Rx Pkts	Tx Pkts	Rx Err	Tx Err
Ethernet Hub	1234567	123456	123456	123456	123456	12345
ATM ADSL 1	1234567	123456	123456	123456	123456	12345
Network	Rx Bytes	Tx Bytes	Rx Pkts	Tx Pkts	Rx Err	Tx Err
IP	1234567	123456	123456	123456	123456	12345
VC Traffic Statistics...						

Physical Interface

The top left side of the screen lists total packets received and total packets transmitted for the following data ports:

- Ethernet
- DSL

Network Interface

The bottom left side of the screen lists total packets received and total packets transmitted:

- IP (IP packets on the Ethernet)

The right side of the table lists the total number of occurrences of each of six types of communication statistics:

- Rx Bytes.** The number of bytes received
- Tx Bytes.** The number of bytes transmitted
- Rx Packets:** The number of packets received
- Tx Pkts.** The number of packets transmitted
- Rx Err:** The number of bad Ethernet packets received
- Tx Err:** The number of errors occurring when Ethernet packets are transmitted simultaneously by nodes on the LAN

System Information

The System Information screen gives a summary view of the general system level values in the Router. From the Statistics & Logs menu select **System Information**. The System Information screen appears.

System Information	
Serial Number	ff-70-00 (16740352)
Firmware Version	8.4
ModelNumber	3341
Processor Speed (Mhz)	50
Flash Rom Capacity (MBytes)	2
DRAM Capacity (MBytes)	16
Hardware Acceleration	Not Installed
Ethernet	Single 10/100 Port
WAN Interface	ADSL

The information display varies by model, firmware version, feature set, and so on. You can tell at a glance your particular system configuration.

Simple Network Management Protocol (SNMP)

The Netopia Firmware Version 8.4 includes a Simple Network Management Protocol (SNMP) agent, allowing monitoring and configuration by a standard SNMP manager. Netopia Routers now support SNMP-V1 and SNMP-V2c.

SNMP Heartbeat Trap

Netopia Firmware Version 8.4 implements a new enterprise-specific SNMP trap, called the heartbeat trap. This has been added to the SNMP MIB file **npaV2trap.mib**. This trap supports the Netopia NetOctopus network monitoring tool.

When enabled, this trap is periodically sent to a management station to confirm that the connection between the device and the management station is still active.

Note that the serialNumber (defined in the netopia/sysParams table) and sysObjectID (defined in the mib-2/system table) values have been included in this trap. The SNMP agent IP address is present in every trap. This information will allow the NetOctopus tool to uniquely identify the device sending the trap.

A single configuration item is required for heartbeat traps – the time interval between traps. Permitted values are 0 – 65535 minutes. A value of zero, the default, means the trap is disabled. Whenever the interval value is set to a non-zero number, a trap is sent immediately and the new (or same) interval value takes effect.

This MIB is available by anonymous ftp from the Netopia ftp server.

MIBs are available in a variety of formats. Load this MIB into your SNMP management software. Follow the instructions included with your SNMP manager on how to load MIBs.

The Netopia Firmware Version 8.4 supports the following management information base (MIB) documents:

- MIB II (RFC 1213)
- Interface MIB (RFC 1229)
- Ethernet MIB (RFC 1643)
- Netopia MIB
- **SNMP-v2 Traps:** SNMP v2 MIB (RFC1907) v2 traps only; NPAV2TRAP.MIB (Netopia-specific)
- **ATM:** ATM TC (RFC2514); ATM MIB (RFC2515)
- **ADSL:** ADSL MIB (RFC2662)

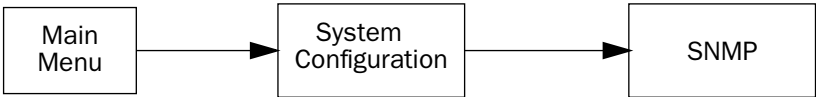
You can obtain the latest SNMP MIBs from the Netopia anonymous FTP server.

FTP to: ***ftp.netopia.com/pub/router/snmpinfo***.

Load these MIBs into your SNMP management software in the order they are listed here. Follow the instructions included with your SNMP manager on how to load MIBs.

The SNMP Setup screen

From the Main Menu, select **SNMP** in the System Configuration screen and press Return. The SNMP Setup screen appears.



SNMP Setup

System Name:

System Location:

System Contact:

System Trap Version:

Read-Only Community String:

Read/Write Community String:

Authentication Traps Enable:

IP Trap Receivers...

SNMP V3 Setup...

+-----+

+-----+

SNMP-V1

SNMP-V2c

+-----+

Off

Follow these steps to configure the first three items in the screen:

1. Select **System Name** and enter a descriptive name for the Router’s SNMP agent.
2. Select **System Location** and enter the gateway’s physical location (room, floor, building, etc.).
3. Select **System Contact** and enter the name of the person responsible for maintaining the gateway.
4. Select the **SNMP Trap Version** and choose either SNMP-V1 or SNMP-V2c. SNMP-V2c is a more feature-rich version, but is not supported by all vendors. Consult with your service provider.

System Name, System Location, and System Contact set the values returned by the Router SNMP agent for the SysName, SysLocation, and SysContact objects, respectively, in the MIB II system group. Although optional, the information you enter in these items can help a system administrator manage the network more efficiently.

Community strings

The **Read-Only Community String** and the **Read/Write Community String** are like passwords that must be used by an SNMP manager querying or configuring the Netopia Firmware Version 8.4. An SNMP manager using the **Read-Only Community String** can examine statistics and configuration information from the gateway, but cannot modify the gateway's configuration. An SNMP manager using the **Read/Write Community String** can both examine and modify configuration parameters.

By default, the read-only and read/write community strings are set to public and private, respectively. You should change both of the default community strings to values known only to you and trusted system administrators.

To change a community string, select it and enter a new value.

Setting the Read-Only and Read-Write community strings to the empty string will block all SNMP requests to the gateway. (The gateway may still send SNMP Traps if those are properly enabled.)

Previously, if either community string was the empty string, SNMP Requests specifying an empty community string were accepted and processed.

This change is designed to allow the administrator to block SNMP access to the gateway and to provide more granular control over the allowed SNMP operations to the gateway.

- Setting only the Read-Write community string to the empty string will block SNMP Set Requests to the gateway, but Get Requests and Get-Next Requests will still be honored using the Read-Only community string (assuming that is not the empty string).
- Setting only the Read-Only community string to the empty string will *not* block Get Requests or Get-Next Requests since those operations (and Set Requests) are still allowed using the (non-empty) Read-Write community string.

Even if you decide not to use SNMP, you should change the community strings. This prevents unauthorized access to the Router through SNMP. For more information on security issues, see [“Suggested Security Measures” on page 9-1](#).

SNMP traps

An SNMP trap is an informational message sent from an SNMP agent (in this case, the Router) to a manager. When a manager receives a trap, it may log the trap as well as generate an alert message of its own.

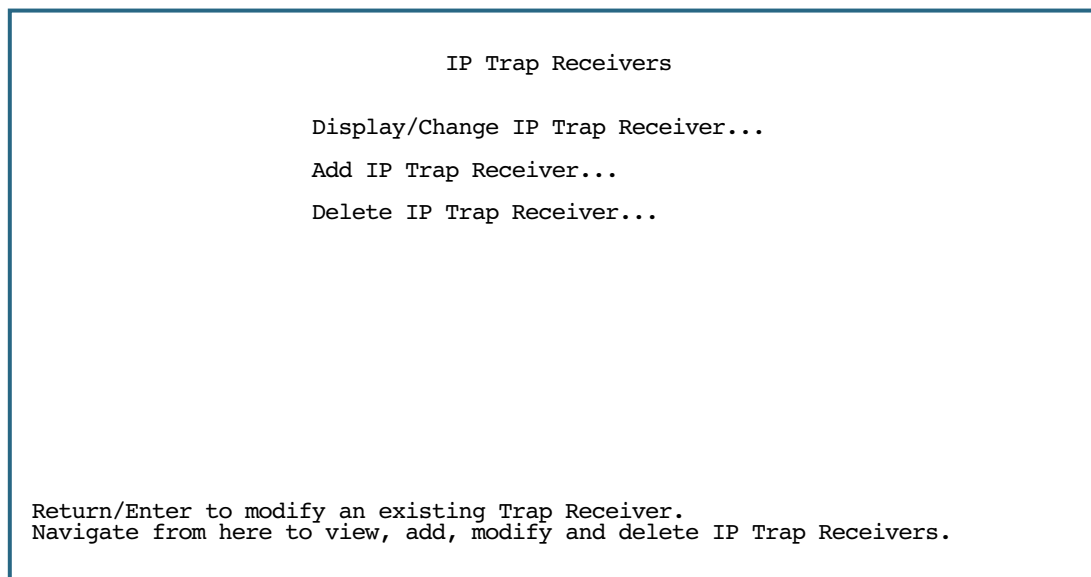
Standard traps generated by the Netopia Firmware Version 8.4 include the following:

- An authentication failure trap is generated when the gateway detects an incorrect community string in a received SNMP packet. **Authentication Traps Enable** must be **On** for this trap to be generated.
- A cold start trap is generated after the gateway is reset.
- An interface down trap (ifDown) is generated when one of the gateway's interfaces, such as a port, stops functioning or is disabled.
- An interface up trap (ifUp) is generated when one of the gateway's interfaces, such as a port, begins functioning.

The Netopia Firmware Version 8.4 sends traps using UDP (for IP networks).

You can specify which SNMP managers are sent the IP traps generated by the Netopia Firmware Version 8.4. Up to eight receivers can be set. You can also review and remove IP traps.

To go to the IP Trap Receivers screen, select **IP Trap Receivers**. The IP Trap Receivers screen appears.



Setting the IP trap receivers

1. Select **Add IP Trap Receiver**.
2. Select **Receiver IP Address or Domain Name**. Enter the IP address or domain name of the SNMP manager you want to receive the trap.
3. Select **Community String** if you enabled one in the SNMP Setup screen, and enter the appropriate password.
4. Select **Add Trap Receiver Now** and press Return. You can add up to seven more receivers.

Viewing IP trap receivers

To display a view-only table of IP trap receivers, select **Display/Change IP Trap Receiver** in the IP Trap Receivers screen.

Modifying IP trap receivers

1. To edit an IP trap receiver, select **Display/Change IP Trap Receiver** in the IP Trap Receivers screen.
2. Select an IP trap receiver from the table and press Return.
3. In the **Change IP Trap Receiver** screen, edit the information as needed and press Return.

Deleting IP trap receivers

1. To delete an IP trap receiver, select **Delete IP Trap Receiver** in the IP Trap Receivers screen.
2. Select an IP trap receiver from the table and press Return.
3. In the dialog box, select **Continue** and press Return.

Chapter 9

Security

The Netopia Firmware Version 8.4 provides a number of security features to help protect its configuration screens and your local network from unauthorized access. Although these features are optional, it is strongly recommended that you use them.

This section covers the following topics:

- [“Suggested Security Measures” on page 9-1](#)
- [“Telnet Tiered Access – Two Password Levels” on page 9-2](#)
- [“Telnet Access” on page 9-16](#)
- [“About Filters and Filter Sets” on page 9-17](#)
- [“Working with IP Filters and Filter Sets” on page 9-24](#)
- [“Policy-based Routing using Filtersets” on page 9-32](#)
- [“Firewall Tutorial” on page 9-35](#)
- [“Configuration Management” on page 9-42](#)

Suggested Security Measures

In addition to setting up user accounts, Telnet access, and filters (all of which are covered later in this chapter), there are other actions you can take to make the Router and your network more secure:

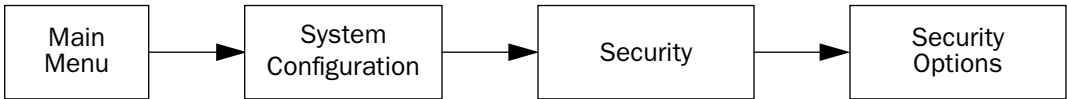
- Change the SNMP community strings (or passwords). The default community strings are universal and could easily be known to a potential intruder.
- Set the answer profile so it must match incoming calls to a connection profile.

Telnet Tiered Access – Two Password Levels

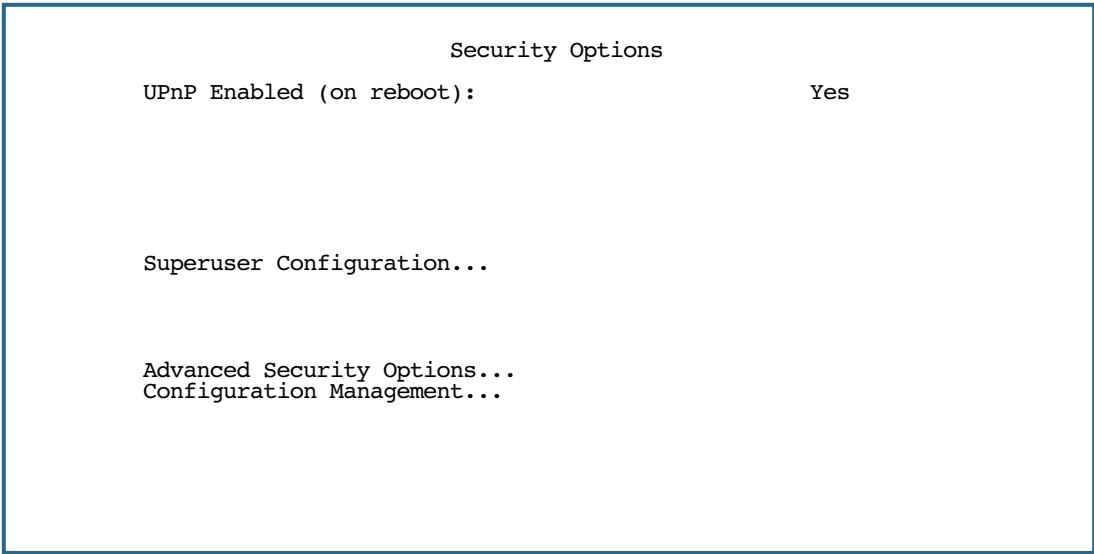
Netopia Firmware Version 8.4 offers tiered access control for greater security and protection against accidental or malicious misconfiguration. Service providers and network administrators can now limit the access of other users to the various configuration screens to prevent misconfigurations.

The access privileges of various users that may be assigned are governed by a *Superuser* administrative account. The Superuser can assign different privileges to *Limited* users who will be accessing the gateway functions in some way.

Configuration access names and passwords are specified in the **Security Options** screen. From the Main Menu, select **System Configuration**, then **Security**.



The **Security Options** screen appears.



UPnP Support

UPnP Enabled: Universal Plug and Play (UPnP™) is a set of protocols that allows a PC to automatically discover other UPnP devices (anything from an internet gateway device to a light switch), retrieve an XML description of the device and its services, control the device, and subscribe to real-time event notification.

By default, UPnP is enabled on the Netopia Gateway.

For Windows XP users, the automatic discovery feature places an icon representing the Netopia Gateway automatically in the “My Network Places” folder.

PCs using UPnP can retrieve the Gateway's WAN IP address, and automatically create NAT port maps. This means that applications that support UPnP, and are used with a UPnP-enabled Netopia Gateway, will not need application layer gateway support on the Netopia Gateway to work through NAT.

You can disable UPnP, if you are not using any UPnP devices or applications.

You must reboot the Netopia device for this setting to take effect.

Superuser configuration

The access privileges of the Superuser account are not modifiable. It is possible, however, to control who can log in as Superuser.

Select **Superuser Configuration** and press **Return**.

The Superuser Configuration screen appears.

Superuser Configuration

Name (19 characters max):	admin
Password:	
Telnet Access Enabled:	Yes
Web Access Enabled:	Yes

ADD SUPERUSERCANCEL

- Assign a Superuser **Name**. It can be up to 19 characters long. It is good practice *not* to use any easily-guessed combination such as your birthday.
 - Assign a **Password**. Keep this password secure. If you lose or forget it, you will not be able to access the gateway without factory defaulting it, thereby losing all of your configuration information.
 - You can disable Telnet or Web Access. This may be useful for extra security in preventing remote attempts to access the gateway.
 - Select **ADD SUPERUSER** and press **Return**. The Superuser account is now configured.
- You will be challenged for this name and password every time you attempt to log into the gateway.

Limited user configuration

The Add Access Name/Password and Show/Change Access Name/Passwords screens allow you to select which configuration features a limited (non-Superuser) user can access. From the Security Options screen, select **Add Access Name/Password**. The Add Access Name/Password screen appears.

Add Access Name/Password

Name (19 characters max):

user

Password:

Telnet Access Enabled:

Yes

Web Access Enabled:

+-----+

Access Privileges...

+-----+
All
LAN
WAN
Custom...
+-----+

ADD USER

CANCEL

- Assign a User Name and Password, and enable or disable Telnet and Web access as in the Superuser Configuration screen.
- Select **Access Privileges**, and from the pull-down menu, choose which access privilege you want this user to have: **All**, **LAN**, or **WAN**.

If you assign any of these privileges, limited users will have full access to privileges associated with these interfaces. You can customize these privileges further, in order to limit access to only certain portions of those interfaces' configuration, by selecting **Custom**. If you select Custom, the **Access Privileges (Custom)** screen appears.

Access Privileges (Custom)

WAN Data Configuration:No

Connection Profile Configuration:No

Circuit (PVC/DLCI) Configuration:No

LAN Data Configuration:Yes

LAN Subnet Configuration:Yes

NAT/Filters Configuration:Yes

Preferences (Global) Configuration:Yes

Voice Configuration:Yes

OK

CANCEL

You can toggle the default user privileges for each user. The defaults are set to minimize the possibility of an individual user inadvertently damaging the WAN connection. Exercise caution in assigning privileges other than these defaults to limited users.

Access Privilege	Default
WAN Data Configuration	No
Connection Profile Configuration	No
Circuit (PVC/DLCI) Configuration	No
LAN Data Configuration	Yes
LAN Subnet Configuration	Yes
NAT/Filters Configuration	Yes
Preferences (Global) Configuration	Yes

Advanced Security Options

The Advanced Security Options screen allows you to configure the global access privileges of users authenticated via a RADIUS server or a TACACS+ server.

From the Security Options screen, select **Advanced Security Options**. The Advanced Security Options screen appears.

RADIUS server authentication

Advanced Security Options

Remote Authentication...
Security Databases...
Remote Server Addr/Name:
Remote Server Secret:
Alt Remote Server Addr/Name:
Alt Remote Server Secret:
RADIUS Identifier:
RADIUS Server Authentication Port

RADIUS
Local only

Remote Access Privileges...

Telnet Server Port:
Device Web Server via LAN only:

All
LAN
WAN
Custom...

LAN (Ethernet) IP Filter Set...
Remove Filter Set

- Select **RADIUS Access Privileges**, and from the pull-down menu, choose which access privilege you want this user to have: **All**, **LAN**, **WAN**, or **Custom**.

If you assign any of these privileges, limited users will have full access to privileges associated with these interfaces. You can customize these privileges further, in order to limit access to only certain portions of those interfaces' configuration, by selecting **Custom**. If you select Custom, the **Access Privileges (Custom)** screen appears.

Access Privileges (Custom)	
WAN Data Configuration:	Yes
Connection Profile Configuration:	Yes
Circuit (PVC/DLCI) Configuration:	Yes
LAN Data Configuration:	Yes
LAN Subnet Configuration:	Yes
NAT/Filters Configuration:	Yes
Preferences (Global) Configuration:	Yes
OK	CANCEL
Return/Enter accepts * Tab toggles * ESC cancels.	

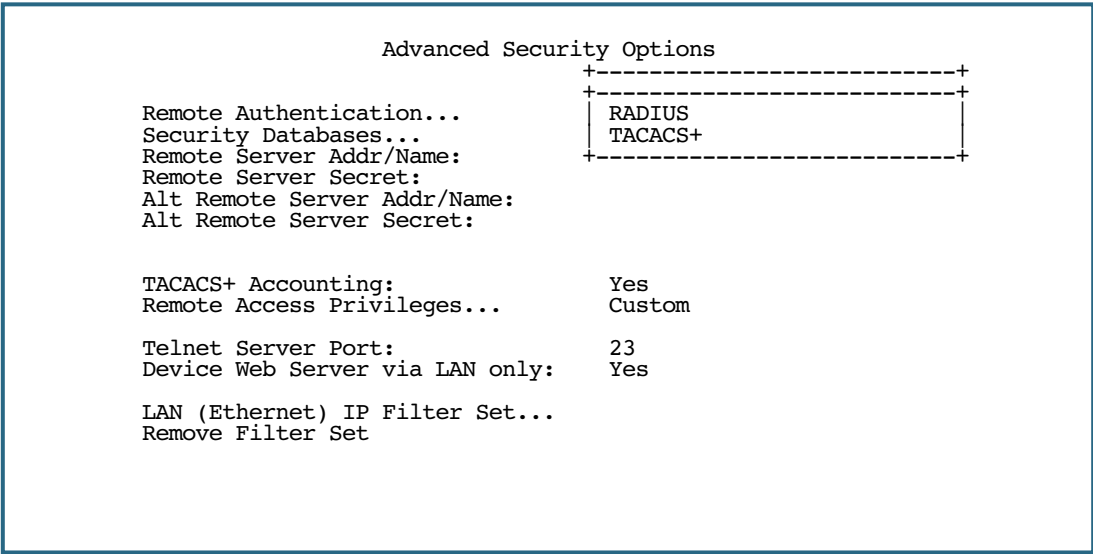
Since authentication via RADIUS server is, by definition, authentication of remote users, the WAN-related defaults are preset to Yes. Toggle any that should be changed.

TACACS+ server authentication

Netopia Firmware Version 8.4 supports TACACS+ server authentication. Its application to a Netopia Router is to control access to the Router’s management interface, and to audit commands submitted by a user.

TACACS (Terminal Access Controller Access Control System) protocol provides access control for Netopia Routers via a centralized server. TACACS+ provides separate authentication, authorization and accounting services.

TACACS allows a client to accept a username and password and query a TACACS authentication server.

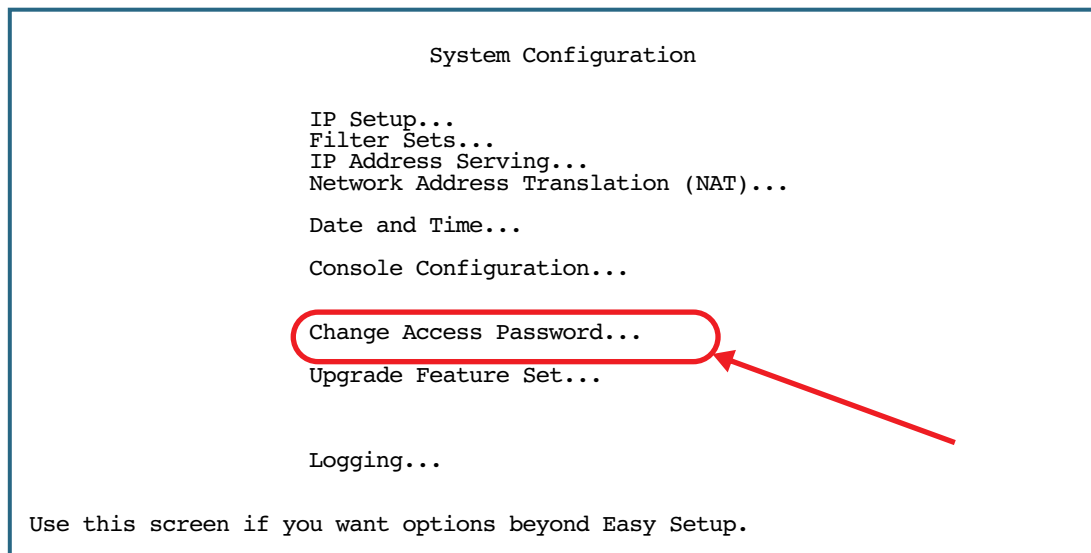


Configuration is similar to RADIUS server configuration. An additional toggle option **TACACS+ Accounting** allows you to enable or disable the TACACS+ Accounting services feature.

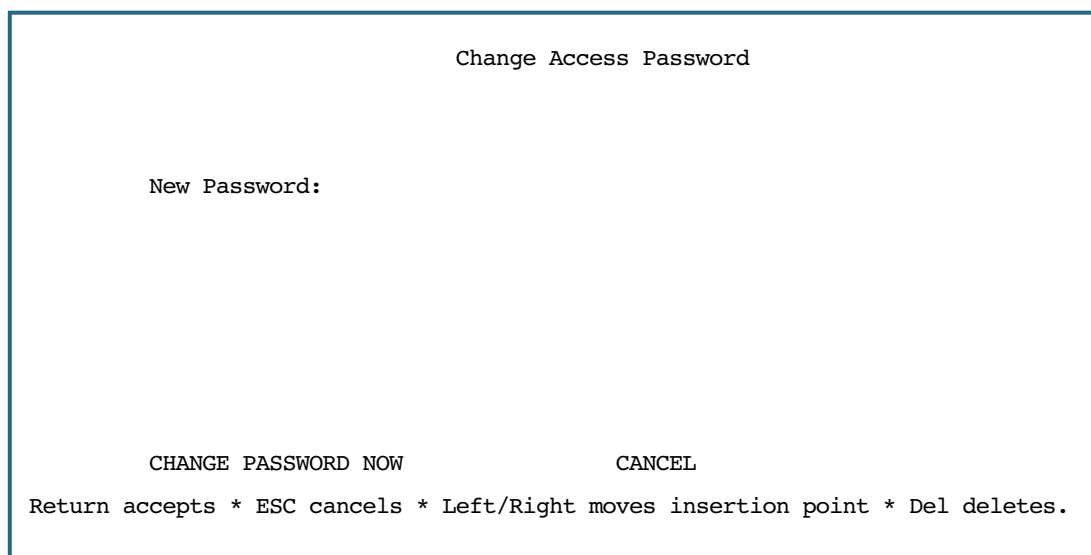
Note: If the user is authenticated by a TACACS+ server, and TACACS+ Accounting is enabled, the session is switched into Command Line Interface (CLI) mode (see the *Command Line Interface Commands Reference*) and cannot be switched to console mode. If TACACS+ Accounting is enabled on the Netopia Router, each command is sent to the TACACS+ server in a TACACS+ Accounting transaction. The CLI command is then executed, regardless of the return code from the server.

User access password

Users must be able to change their names and passwords, regardless of other security access restrictions. If a user does not have security access, then they will only be able to modify the password for their account. When a limited-access user logs into the gateway. and accesses the System Configuration menus, the only Security option displayed is **Change Access Password**.



Selecting this option displays the **Change Access Password** screen.



When changing a password, you will be challenged to enter it again to be sure you have entered it correctly.

User menu differences

Menus reflect the security access level of the user. Consequently, configuration menus will display differing options based upon the parameters a particular user is allowed to change. Some differences include:

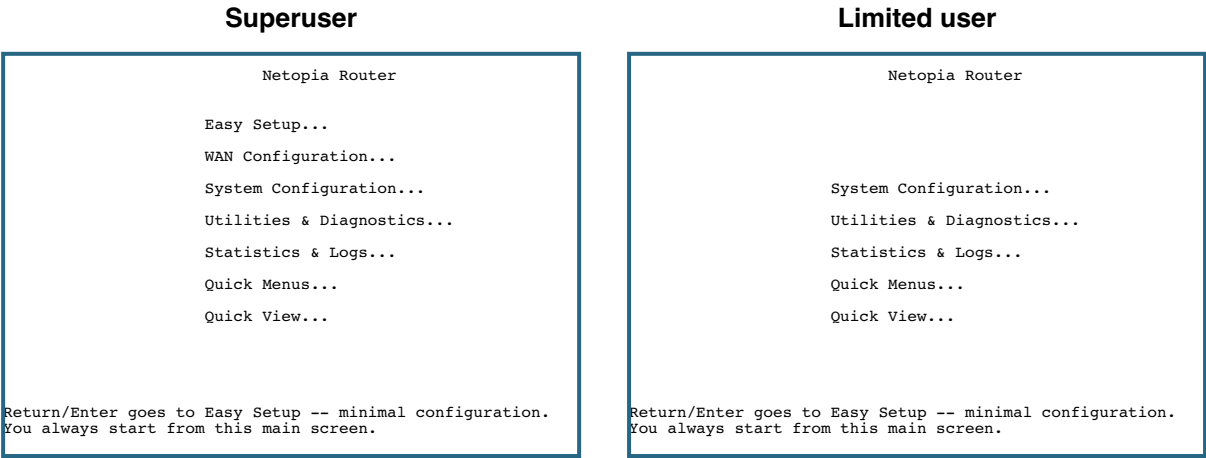
- Limited users (non-Superusers) do not have access to Easy Setup.

9-10 Firmware User Guide

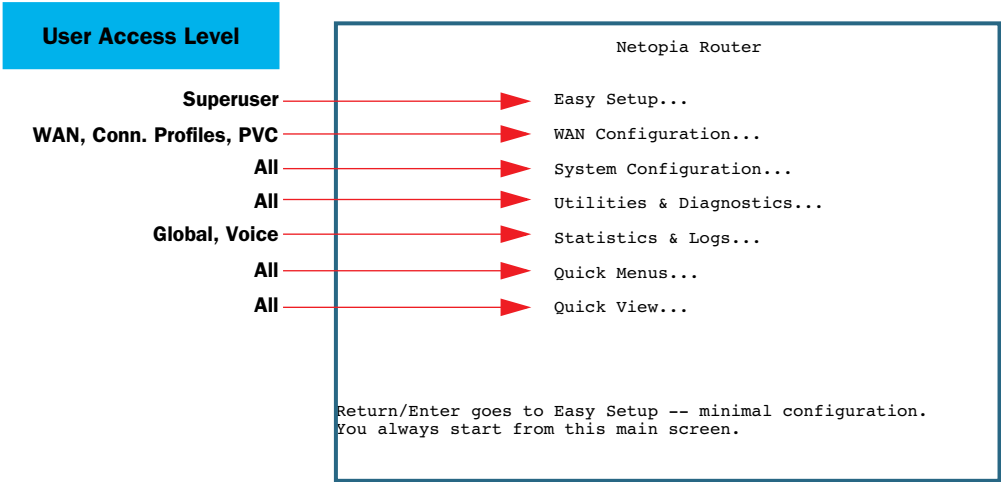
- All users have access to System Configuration, Quick Menu, and Quick View, but limited users have only limited access to configuration elements in their descendant menus.
- Configuration screen elements to which configuration access is forbidden are usually hidden.
- The Quick Menu screen reflects the security access level of the user. Menus to which configuration access is forbidden are hidden.

Main Menu

The following is an example comparison of the Main Menu as seen by the Superuser and by a Limited user.

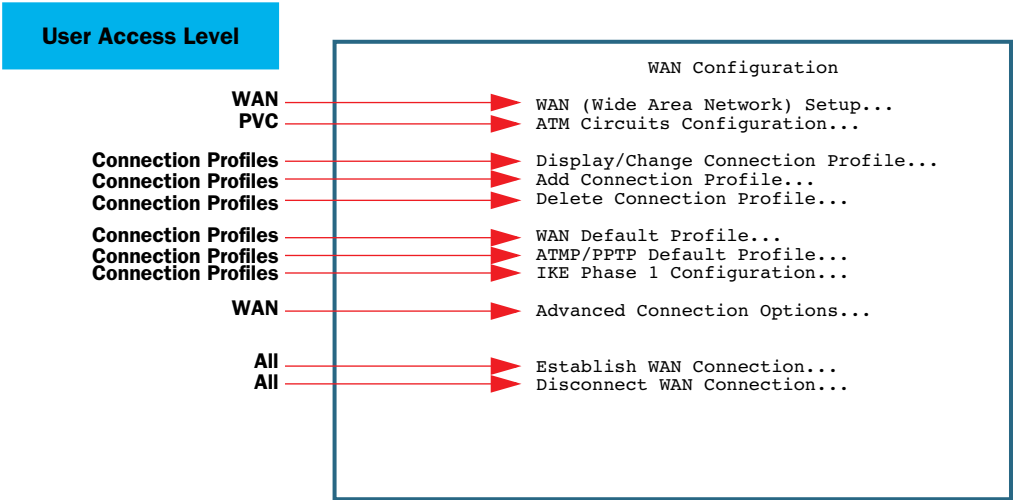


Based on access level, the Main Menu displays its configuration options according to the following diagram:

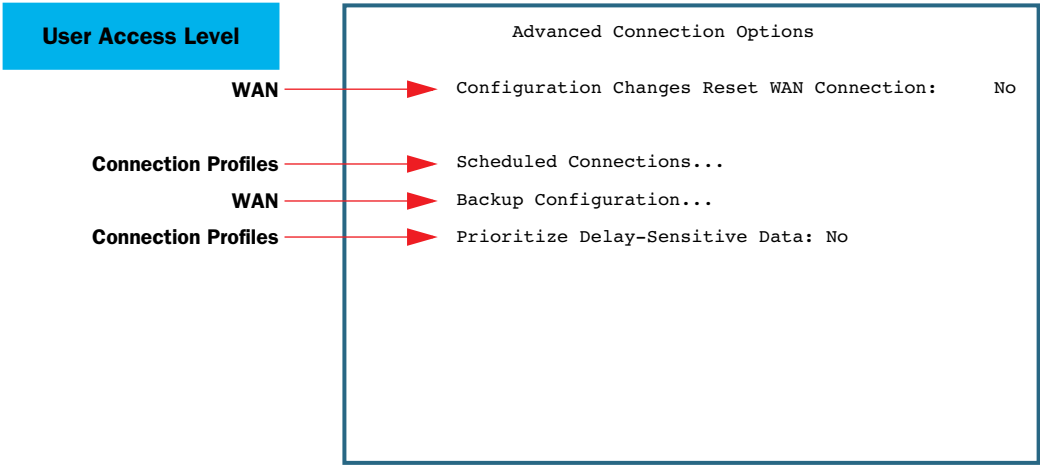


WAN Configuration screens

If a limited user is allowed WAN, Connection Profile, or PVC configuration access, the WAN Configuration option in the Main Menu is visible. If a limited user selects **WAN Configuration** in the Main Menu, the WAN Configuration screen displays its configuration options according to the following diagram:



If a limited user selects **Advanced Connection Options** in the WAN Configuration menu, the Advanced Connection Options screen displays its configuration options according to the following diagram:



Connection Profiles

The Superuser can disallow limited user access to a particular Connection Profile. When adding a Connection Profile in the Add Connection Profile screen the Superuser can toggle the **Superuser Accessible Only** option to **Yes** or **No**.

Add Connection Profile

Profile Name:Profile 1

Profile Enabled:Yes

Encapsulation Type...PPP

Encapsulation Options...

IP Profile Parameters...

Superuser Accessible Only:No

COMMIT

CANCEL

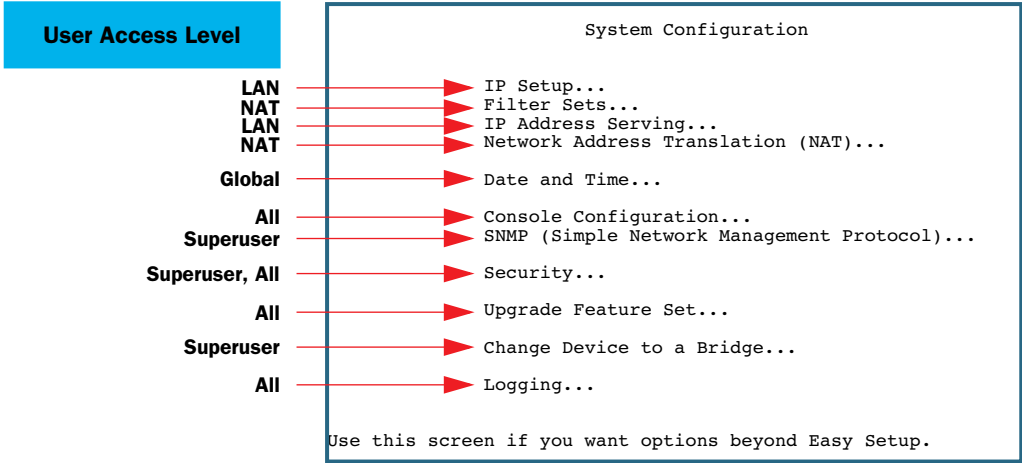
Return/Enter to accept the profile.

Configure a new Conn. Profile. Finished? COMMIT or CANCEL to exit.

This option is visible whether or not there are authorized username/passwords other than the Superuser. The Superuser can also change the user accessibility after creating a Connection Profile or a limited user in the **Change Connection Profile** screen.

System Configuration menu

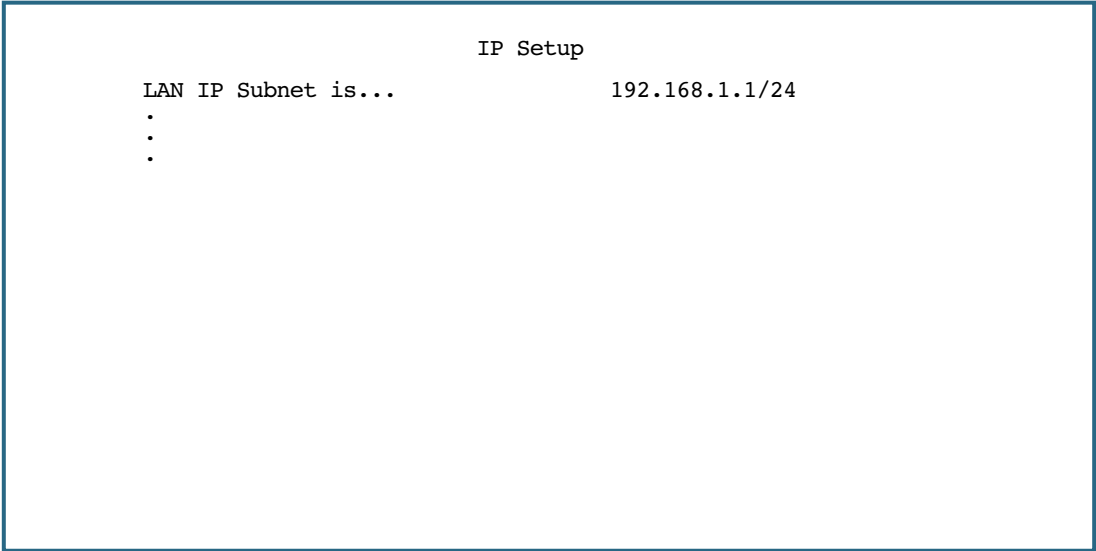
The System Configuration menu is always available to all users. Based on access level, the System Configuration menu displays its configuration options according to the following diagram:



Note: Network Address Translation (NAT) is displayed in this screen in order to make access control simpler. **Security** becomes **Change Access Password** for non-Superusers, and provides access to the associated menu described previously.

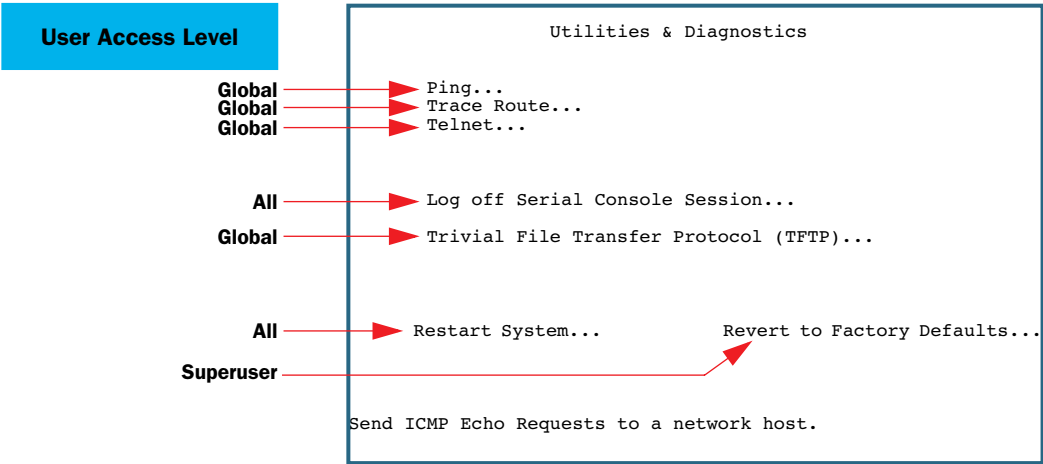
IP Setup menu

In the IP Setup menu, users that do not have LAN Subnet Configuration access will see a screen similar to the following:



Utilities & Diagnostics menu

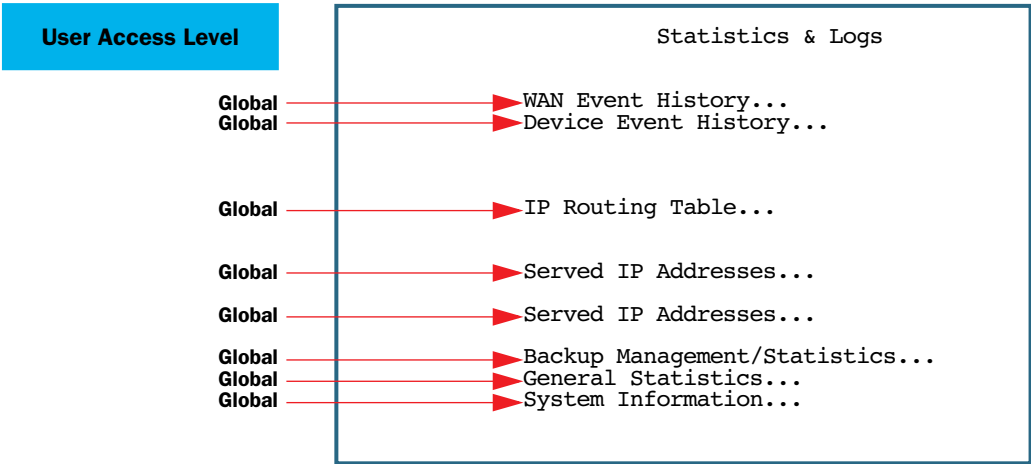
Based on access level, the Utilities & Diagnostics menu displays its configuration options according to the following diagram:



Statistics & Logs menu

The Statistics & Logs menu shown below is a composite of all the possible options on all Netopia gateways supported by the firmware. Substantial differences exist among screens on a given gateway. Here, all selection options are shown.

Based on access level, the Statistics & Logs menu displays its options according to the following diagram:



Quick Menu

Quick Menus vary considerably between models, features, and access levels. The following is an example comparison of the Quick Menu as seen by the Superuser and by a Limited user.

Superuser

Quick Menu

Connection Profiles

Add Connection Profiles

Change Connection Profiles

Delete Connection Profiles

WAN Default Profile

ATMP/PPTP Default Profile

IKE Phase 1 Config

Scheduled Connections

Add Scheduled Connection

Change Scheduled Connection

Delete Scheduled Connection

Console Configuration

SNMP Setup

Line Configuration

Fr. Relay Config

Fr. Relay DLCI Config

Backup Config

Telephone Setup

MacIP Setup

TFTP

IP Setup

IP Address Serving Setup

IP Filter Sets

Static Routes

Network Address Translation

Limited user

Quick Menu

IP Setup

IP Address Serving Setup

Filter Sets

Static Routes

Network Address Translation

Console Configuration

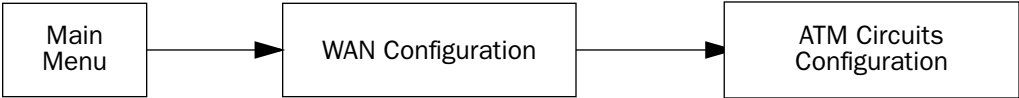
TFTP

This menu allows you to visit most configuration screens.

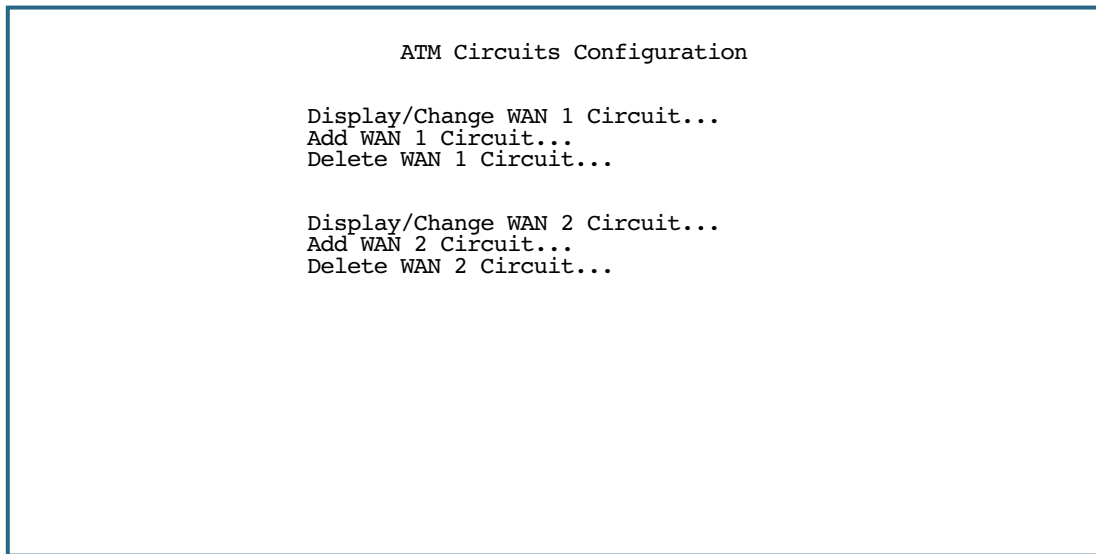
Note: Console Configuration is always visible.

ATM Circuits Configuration menu

You select **ATM Circuits Configuration** from the WAN Configuration menu.



The ATM Circuits Configuration menu screen appears as follows:



Note: Multiple ATM circuit configuration is supported on multiple ATM-capable gateways. Although some of the parameters of the Circuit Configuration screens pertain to Voice and Connection Profiles, it is assumed that if the user has been granted PVC configuration access, they are permitted configuration access to all PVC parameters.

Telnet Access

Telnet is a TCP/IP service that allows remote terminals to access hosts on an IP network. Netopia Firmware Version 8.4 supports Telnet access to its configuration screens.

Caution!

You should consider password-protecting or restricting Telnet access to the Router if you suspect there is a chance of tampering.

To password-protect the configuration screens, select Easy Setup from the Main Menu, and go to the Easy Setup Security Configuration screen. By entering a name and password pair in this screen, all access via Telnet and SNMP will be password-protected.

To restrict Telnet access, select **Security** in the Advanced Configuration menu. The Security Options screen will appear. There are two levels of Telnet restriction available:

- To restrict Telnet access to the SNMP screens, select **Enable Telnet Access to SNMP Screens** and toggle it to **No**. (See “SNMP traps” on page 8-12.)
- To restrict Telnet access to all of the configuration screens, select **Enable Telnet Console Access** and toggle it to **No**.

About Filters and Filter Sets

Security should be a high priority for anyone administering a network connected to the Internet. Using packet filters to control network communications can greatly improve your network's security.

The Netopia Firmware Version 8.4's packet filters are designed to provide security for the Internet connections made to and from your network. You can customize the gateway's filter sets for a variety of packet filtering applications. Typically, you use filters to selectively admit or refuse TCP/IP connections from certain remote networks and specific hosts. You will also use filters to screen particular types of connections. This is commonly called *firewalling* your network.

Before creating filter sets, you should read the next few sections to learn more about how these powerful security tools work.

What's a filter and what's a filter set?

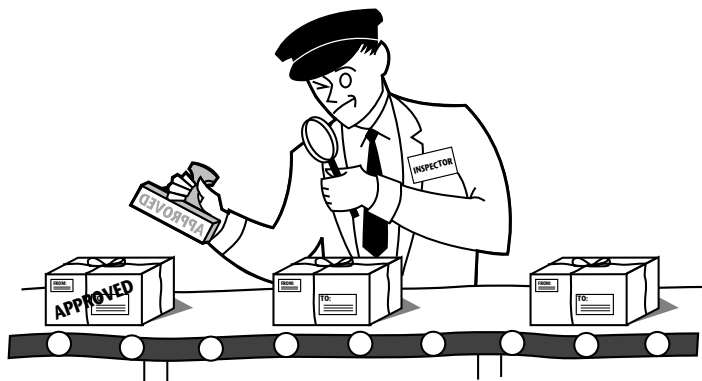
A filter is a rule that lets you specify what sort of data can flow in and out of your network. A particular filter can be either an input filter—one that is used on data (packets) coming in to your network from the Internet—or an output filter—one that is used on data (packets) going out from your network to the Internet.

A filter set is a group of filters that work together to check incoming or outgoing data. A filter set can consist of a combination of input and output filters.

How filter sets work

A filter set acts like a team of customs inspectors. Each filter is an inspector through which incoming and outgoing packages must pass. The inspectors work as a team, but each inspects every package individually.

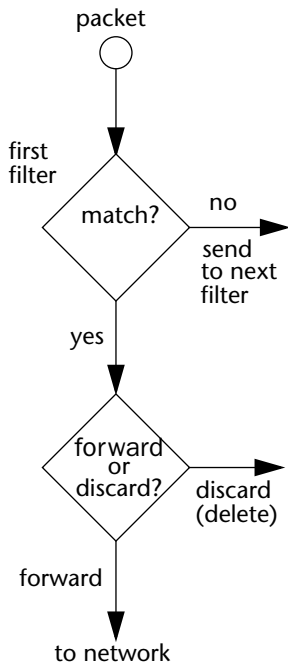
Each inspector has a specific task. One inspector's task may be to examine the destination address of all outgoing packages. That inspector looks for a certain destination—which could be as specific as a street address or as broad as an entire country—and checks each package's destination address to see if it matches that destination.



A filter inspects data packets like a customs inspector scrutinizing packages.

Filter priority

Continuing the customs inspectors analogy, imagine the inspectors lined up to examine a package. If the package matches the first inspector's criteria, the package is either rejected or passed on to its destination, depending on the first inspector's particular orders. In this case, the package is never seen by the remaining inspectors.



If the package does not match the first inspector's criteria, it goes to the second inspector, and so on. You can see that the order of the inspectors in the line is very important.

For example, let's say the first inspector's orders are to send along all packages that come from Rome, and the second inspector's orders are to reject all packages that come from France. If a package arrives from Rome, the first inspector sends it along without allowing the second inspector to see it. A package from Paris is ignored by the first inspector, rejected by the second inspector, and never seen by the others. A package from London is ignored by the first two inspectors, so it's seen by the third inspector.

In the same way, filter sets apply their filters in a particular order. The first filter applied can forward or discard a packet before that packet ever reaches any of the other filters. If the first filter can neither forward nor discard the packet (because it cannot match any criteria), the second filter has a chance to forward or reject it, and so on. Because of this hierarchical structure, each filter is said to have a priority. The first filter has the highest priority, and the last filter has the lowest priority.

How individual filters work

As described above, a filter applies criteria to an IP packet and then takes one of three actions:

- Forwards the packet to the local or remote network

- Blocks (discards) the packet
- Ignores the packet

A filter forwards or blocks a packet only if it finds a match after applying its criteria. When no match occurs, the filter ignores the packet.

A filtering rule

The criteria are based on information contained in the packets. A filter is simply a rule that prescribes certain actions based on certain conditions. For example, the following rule qualifies as a filter:

Block all Telnet attempts that originate from the remote host 199.211.211.17.

This rule applies to Telnet packets that come from a host with the IP address 199.211.211.17. If a match occurs, the packet is blocked.

Here is what this rule looks like when implemented as a filter on the Netopia Firmware Version 8.4:

+--#--Source IP Addr--Dest IP Addr-----Proto--Src.Port--D.Port--On?--Fwd--+
1 199.211.211.17 0.0.0.0 TCP 23 Yes No
+-----+-----+-----+-----+-----+-----+-----+-----+-----+

To understand this particular filter, look at the parts of a filter.

Parts of a filter

A filter consists of criteria based on packet attributes. A typical filter can match a packet on any one of the following attributes:

- The source IP address (where the packet was sent from)
- The destination IP address (where the packet is going)
- The type of higher-layer Internet protocol the packet is carrying, such as TCP or UDP

Port numbers

A filter can also match a packet's port number attributes, but only if the filter's protocol type is set to TCP or UDP, since only those protocols use port numbers. The filter can be configured to match the following:

- The source port number (the port on the sending host that originated the packet)
- The destination port number (the port on the receiving host that the packet is destined for)

By matching on a port number, a filter can be applied to selected TCP or UDP services, such as Telnet, FTP, and World Wide Web. The following tables show a few common services and their associated port numbers:

Internet service	TCP port	Internet service	TCP port
FTP	20/21	Finger	79
Telnet	23	World Wide Web	80

Internet service	TCP port	Internet service	TCP port
SMTP (mail)	25	News	144
Gopher	70	rlogin	513

Internet service	UDP port	Internet service	UDP port
Who Is	43	AppleTalk Routing Maintenance (at-rtmp)	202
World Wide Web	80	AppleTalk Name Binding (at-nbp)	202
SNMP	161	AURP (AppleTalk)	387
TFTP	69	who	513

Port number comparisons

A filter can also use a comparison option to evaluate a packet's source or destination port number. The comparison options are:

No Compare: No comparison of the port number specified in the filter with the packet's port number.

Not Equal To: For the filter to match, the packet's port number cannot equal the port number specified in the filter.

Less Than: For the filter to match, the packet's port number must be less than the port number specified in the filter.

Less Than or Equal: For the filter to match, the packet's port number must be less than or equal to the port number specified in the filter.

Equal: For the filter to match, the packet's port number must equal the port number specified in the filter.

Greater Than: For the filter to match, the packet's port number must be greater than the port number specified in the filter.

Greater Than or Equal: For the filter to match, the packet's port number must be greater than or equal to the port number specified in the filter.

Other filter attributes

There are three other attributes to each filter:

- The filter's order (i.e., priority) in the filter set
- Whether the filter is currently active
- Whether the filter is set to forward packets or to block (discard) packets

Putting the parts together

When you display a filter set, its filters are displayed as rows in a table:

+ #	Source IP Addr	Dest IP Addr	Proto	Src.Port	D.Port	On?	Fwd?
1	192.211.211.17	0.0.0.0	TCP	0	23	Yes	No
2	0.0.0.0	0.0.0.0	TCP	NC	=6000	Yes	No
3	0.0.0.0	0.0.0.0	ICMP	--	--	Yes	Yes
4	0.0.0.0	0.0.0.0	TCP	NC	>1023	Yes	Yes
5	0.0.0.0	0.0.0.0	UDP	NC	>1023	Yes	Yes

The table’s columns correspond to each filter’s attributes:

#: The filter’s priority in the set. Filter number 1, with the highest priority, is first in the table.

Source IP Addr: The packet source IP address to match.

Dest IP Addr: The packet destination IP address to match.

Proto: The protocol to match. This can be entered as a number (see the table below) or as TCP or UDP if those protocols are used.

Protocol	Number to use	Full name
N/A	0	Ignores protocol type
ICMP	1	Internet Control Message Protocol
TCP	6	Transmission Control Protocol
UDP	17	User Datagram Protocol

Src. Port: The source port to match. This is the port on the sending host that originated the packet.

D. Port: The destination port to match. This is the port on the receiving host for which the packet is intended.

On?: Displays **Yes** when the filter is in effect or **No** when it is not.

Fwd: Shows whether the filter forwards (**Yes**) a packet or discards (**No**) it when there’s a match.

Filtering example #1

Returning to our filtering rule example from above (see [page 9-19](#)), look at how a rule is translated into a filter. Start with the rule, then fill in the filter's attributes:

1. The rule you want to implement as a filter is:
Block all Telnet attempts that originate from the remote host 199.211.211.17.
2. The host 199.211.211.17 is the source of the Telnet packets you want to block, while the destination address is any IP address. How these IP addresses are masked determines what the final match will be, although the mask is not displayed in the table that displays the filter sets (you set it when you create the filter). In fact, since the mask for the destination IP address is 0.0.0.0, the address for Dest IP Addr could have been anything. The mask for Source IP Addr must be 255.255.255.255 since an exact match is desired.
 - Source IP Addr = 199.211.211.17
 - Source IP address mask = 255.255.255.255
 - Dest IP Addr = 0.0.0.0
 - Destination IP address mask = 0.0.0.0
3. Using the tables on [page 9-19](#), find the destination port and protocol numbers (the *local* Telnet port):
 - Proto = TCP (or 6)
 - D. Port = 23
4. The filter should be enabled and instructed to block the Telnet packets containing the source address shown in step 2:
 - On? = Yes
 - Fwd = No

This four-step process is how we produced the following filter from the original rule:

+ #	Source IP Addr	Dest IP Addr	Proto	Src.Port	D.Port	On?	Fwd
1	192.211.211.17	0.0.0.0	TCP	0	23	Yes	No

Filtering example #2

Suppose a filter is configured to block all incoming IP packets with the source IP address of 200.233.14.0, regardless of the type of connection or its destination. The filter would look like this:

+ #	Source IP Addr	Dest IP Addr	Proto	Src.Port	D.Port	On?	Fwd
1	200.233.14.0	0.0.0.0	0			Yes	No

This filter blocks any packets coming from a remote network with the IP network address 200.233.14.0. The 0 at the end of the address signifies *any* host on the class C IP network 200.233.14.0. If, for example, the filter is applied to a packet with the source IP address 200.233.14.5, it will block it.

In this case, the mask, which does not appear in the table, must be set to 255.255.255.0. This way, all packets with a source address of 200.233.14.x will be matched correctly, no matter what the final address byte is.

Note: The protocol attribute for this filter is 0 by default. This tells the filter to ignore the IP protocol or type of IP packet.

Design guidelines

Careful thought must go into designing a new filter set. You should consider the following guidelines:

- Be sure the filter set's overall purpose is clear from the beginning. A vague purpose can lead to a faulty set, and that can actually make your network *less* secure.
- Be sure each individual filter's purpose is clear.
- Determine how filter priority will affect the set's actions. Test the set (on paper) by determining how the filters would respond to a number of different hypothetical packets.
- Consider the combined effect of the filters. If every filter in a set fails to match on a particular packet, the packet is:
 - Forwarded if all the filters are configured to discard (*not* forward)
 - Discarded if all the filters are configured to forward
 - Discarded if the set contains a combination of forward and discard filters

Disadvantages of filters

Although using filter sets can greatly enhance network security, there are disadvantages:

- Filters are complex. Combining them in filter sets introduces subtle interactions, increasing the likelihood of implementation errors.
- Enabling a large number of filters can have a negative impact on performance. Processing of packets will take longer if they have to go through many checkpoints.
- Too much reliance on packet filters can cause too little reliance on other security methods. Filter sets are *not* a substitute for password protection, effective safeguarding of passwords, caller ID, the "must match" option in the answer profile, PAP or CHAP in connection profiles, callback, and general awareness of how your network may be vulnerable.

An approach to using filters

The ultimate goal of network security is to prevent unauthorized access to the network without compromising authorized access. Using filter sets is part of reaching that goal.

Each filter set you design will be based on one of the following approaches:

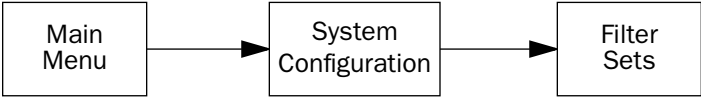
- That which is not expressly prohibited is permitted.

- That which is not expressly permitted is prohibited.

It is strongly recommended that you take the latter, and safer, approach to all of your filter set designs.

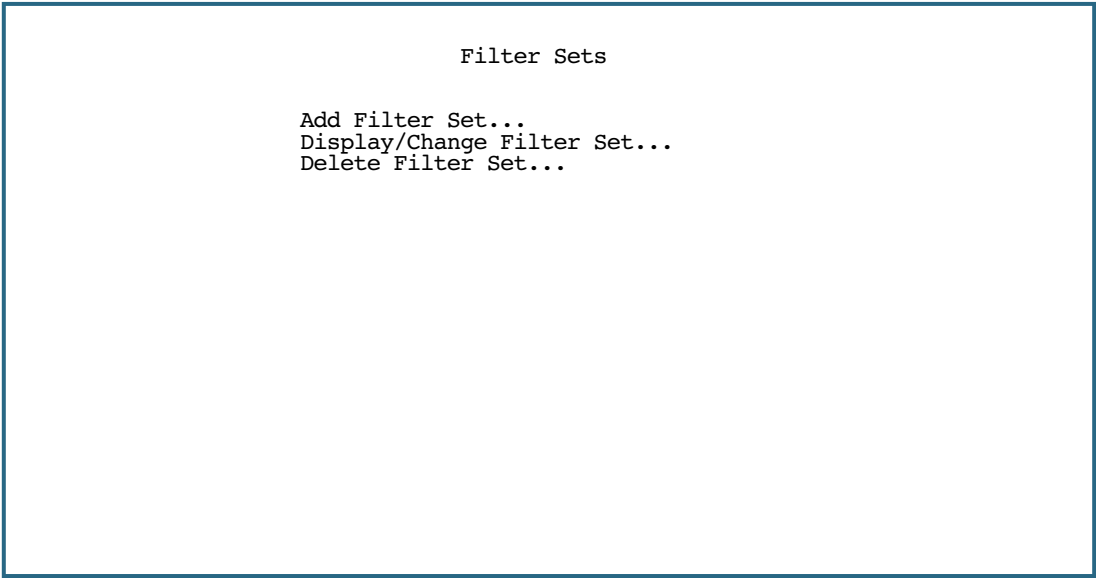
Working with IP Filters and Filter Sets

This section covers IP filters and filter sets.



To work with filters and filter sets, begin by accessing the filter set screens.

Note: Make sure you understand how filters work before attempting to use them. Read the section [“About Filters and Filter Sets,” beginning on page 9-17.](#)



The procedure for creating and maintaining filter sets is as follows:

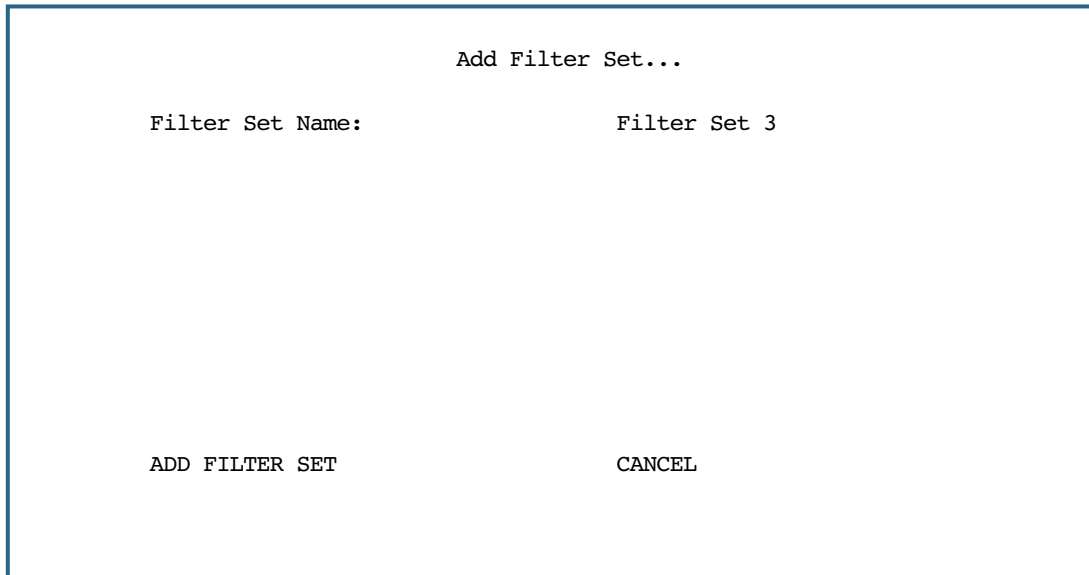
1. Add a new filter set.
2. Create the filters for the new filter set.
3. View, change, or delete individual filters and filter sets.

The sections below explain how to execute these steps.

Adding a filter set

You can create up to eight different custom filter sets. Each filter set can contain up to 16 output filters and up to 16 input filters.

To add a new filter set, select **Add Filter Set** in the Filter Sets screen and press Return. The Add Filter Set screen appears.



Add Filter Set...

Filter Set Name: Filter Set 3

ADD FILTER SET CANCEL

Naming a new filter set

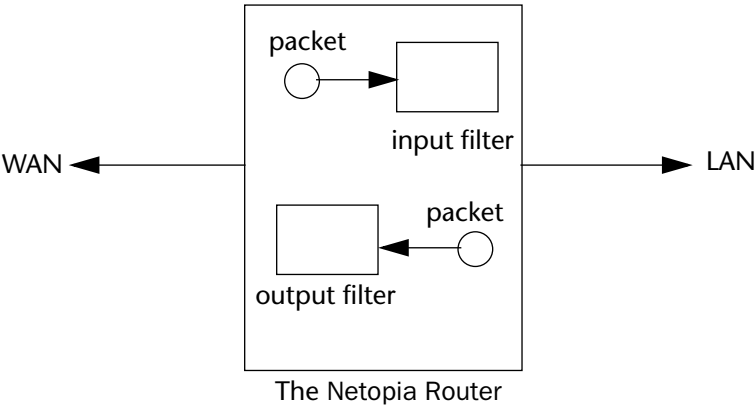
All new filter sets have a default name. The first filter set you add will be called Filter Set 1, the next filter will be Filter Set 2, and so on.

To give a new filter set a different name, select **Filter Set Name** and enter a new name for the filter set.

To save the filter set, select **ADD FILTER SET**. The saved filter set is empty (contains no filters), but you can return to it later to add filters (see [“Adding filters to a filter set” on page 9-26](#)).

Adding filters to a filter set

There are two kinds of filters you can add to a filter set: input and output. Input filters check packets received from the Internet, destined for your network. Output filters check packets transmitted from your network to the Internet.



Packets in the Netopia Firmware Version 8.4 pass through an input filter if they originate in the WAN and through an output filter if they're being sent out to the WAN.

The process for adding input and output filters is exactly the same. The main difference between the two involves their reference to source and destination. From the perspective of an input filter, your local network is the destination of the packets it checks, and the remote network is their source. From the perspective of an output filter, your local network is the source of the packets, and the remote network is their destination.

Type of filter	Source means	Destination means
Input filter	The remote network	The local network
Output filter	The local network	The remote network

To add a filter, select **Display/Change Filter Set** in the Filter Set screen. From the pop-up menu, select the filter set to which you will add a filter. The Display/Change Filter Set screen appears.

Display/Change Filter Set...	
Filter Set Name:	Filter Set 3
Add Input Filter to Filter Set... Display/Change Input Filter... Delete Input Filter... Move Input Filter...	
Add Output Filter to Filter Set... Display/Change Output Filter... Delete Output Filter... Move Output Filter...	

Note: There are two groups of items in this screen, one for input filters and one for output filters. In this section, you'll learn how to add an input filter to a filter set. Adding an output filter works exactly the same way, providing you keep the different source and destination perspectives in mind.

1. To add a filter, select **Add Input Filter to Filter Set** and press Return. The Add Input Filter screen appears.

Add Input Filter	
Enabled:	Yes
Forward:	No
Source IP Address:	0.0.0.0
Source IP Address Mask:	0.0.0.0
Dest. IP Address:	0.0.0.0
Dest. IP Address Mask:	0.0.0.0
Protocol Type:	ANY
Protocol Type:	TCP
Source Port Compare...	No Compare
Source Port ID:	0
Dest. Port Compare...	No Compare
Dest. Port ID:	0
Established TCP Conns. Only:	No
ADD THIS FILTER NOW	CANCEL

2. To make the filter active in the filter set, select **Enabled** and toggle it to **Yes**. If **Enabled** is toggled to **No**, the filter can still exist in the filter set, but it will have no effect.

3. If you want the filter to forward packets that match its criteria to the destination IP address, select **Forward** and toggle it to **Yes**. If **Forward** is toggled to **No**, packets matching the filter's criteria will be discarded.
4. Select **Source IP Address** and enter the source IP address this filter will match on. You can enter a subnet or a host address.
5. Select **Source IP Address Mask** and enter a mask for the source IP address. This allows you to further modify the way the filter will match on the source address. Enter 0.0.0.0 to force the filter to match on all source IP addresses, or enter 255.255.255.255 to match the source IP address exclusively.
6. Select **Dest. IP Address** and enter the destination IP address this filter will match on. You can enter a subnet or a host address.
7. Select **Dest. IP Address Mask** and enter a mask for the destination IP address. This allows you to further modify the way the filter will match on the destination address. Enter 0.0.0.0 to force the filter to match on all destination IP addresses.
8. Select **Protocol Type** and enter **ICMP, TCP, UDP, Any**, or the number of another IP transport protocol (see the table on [page 9-21](#)).

Note: If Protocol Type is set to TCP or UDP, the settings for port comparison that you configure in steps 8 and 9 will appear. These settings only take effect if the Protocol Type is TCP or UDP.

9. Select **Source Port Compare** and choose a comparison method for the filter to use on a packet's source port number. Then select **Source Port ID** and enter the actual source port number to match on (see the table on [page 9-19](#)).
10. Select **Dest. Port Compare** and choose a comparison method for the filter to use on a packet's destination port number. Then select **Dest. Port ID** and enter the actual destination port number to match on (see the table on [page 9-19](#)).
11. When you are finished configuring the filter, select **ADD THIS FILTER NOW** to save the filter in the filter set. Select **CANCEL** to discard the filter and return to the Add IP Filter Set screen.

Viewing filters

To display a table of input or output filters, select **Display/Change Input Filter** or **Display/Change Output Filter** in the Display/Change Filter Set screen.

Modifying filters

To modify a filter, select **Display/Change Input Filter** or **Display/Change Output Filter** in the Display/Change Filter Set screen. Select a filter from the table and press Return. The Change Filter screen appears. The parameters in this screen are set in the same way as the ones in the Add Filter screen (see [“Adding filters to a filter set” on page 9-26](#)).

Change Filter

Enabled:	No
Forward:	No
Source IP Address:	0.0.0.0
Source IP Address Mask:	0.0.0.0
Dest. IP Address:	0.0.0.0
Dest. IP Address Mask:	0.0.0.0
Protocol Type:	0
Source Port Compare...	No Compare
Source Port ID:	0
Dest. Port Compare...	No Compare
Dest. Port ID:	0

Enter the IP specific information for this filter.

Deleting filters

To delete a filter, select **Delete Input Filter** or **Delete Output Filter** in the Display/Change Filter Set screen to display a table of filters.

Select the filter from the table and press Return to delete it. Press Escape to exit the table without deleting the filter.

Moving filters

To reorganize the filters in a filter set, select **Move Input Filter** or **Move Output Filter** in the Display/Change Filter Set screen to display a table of filters.

Select a filter from the table and press Return. Then use the up or down arrow key to change the filter’s order in the filter set. Press Return to accept the new filter location.

Deleting a filter set

Note: If you delete a filter set, all of the filters it contains are deleted as well. To reuse any of these filters in another set, before deleting the current filter set you’ll have to note their configuration and then recreate them.

To delete a filter set, select **Delete Filter Set** in the Filter Sets screen to display a list of filter sets.

Select a filter set from the list and press Return. Select CONTINUE and press Return to delete it.

A sample filter set

This section contains the settings for a filter set called Basic Firewall, which is part of the Netopia Firmware Version 8.4’s factory configuration.

Basic Firewall blocks undesirable traffic originating from the WAN (in most cases, the Internet), but forwards all traffic originating from the LAN. It follows the conservative “that which is not expressly permitted is prohibited” approach: unless an incoming packet expressly matches one of the constituent input filters, it will not be forwarded to the LAN.

The five input filters and one output filter that make up Basic Firewall are shown in the table below.

Setting	Input filter 1	Input filter 2	Input filter 3	Input filter 4	Input filter 5	Output filter 1
Enabled	Yes	Yes	Yes	Yes	Yes	Yes
Forward	No	No	Yes	Yes	Yes	Yes
Source IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Source IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Dest. IP address mask	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Protocol type	TCP	TCP	ICMP	TCP	UDP	0
Source port comparison	No Compare	No Compare	N/A	No Compare	No Compare	N/A
Source port ID	0	0	N/A	0	0	N/A
Dest. port comparison	Equal	Equal	N/A	Greater Than	Greater Than	N/A
Dest. port ID	2000	6000	N/A	1023	1023	N/A

Basic Firewall’s filters play the following roles.

Input filters 1 and 2: These block WAN-originated OpenWindows and X-Windows sessions. Service origination requests for these protocols use ports 2000 and 6000, respectively. Since these are greater than 1023, OpenWindows and X-Windows traffic would otherwise be allowed by input filter 4. Input filters 1 and 2 must precede input filter 4; otherwise they would have no effect since filter 4 would have already forwarded OpenWindows and X-Windows traffic.

Input filter 3: This filter explicitly forwards all WAN-originated ICMP traffic to permit devices on the WAN to ping devices on the LAN. Ping is an Internet service that is useful for diagnostic purposes.

Input filters 4 and 5: These filters forward all TCP and UDP traffic, respectively, when the destination port is greater than 1023. This type of traffic generally does not allow a remote host to connect to the LAN using one of the potentially intrusive Internet services, such as Telnet, FTP, and WWW.

Output filter 1: This filter forwards all outgoing traffic to make sure that no outgoing connections from the LAN are blocked.

Basic Firewall is suitable for a LAN containing only client hosts that want to access servers on the WAN, but not for a LAN containing servers providing services to clients on the WAN. Basic Firewall's general strategy is to explicitly forward WAN-originated TCP and UDP traffic to ports greater than 1023. Ports lower than 1024 are the service origination ports for various Internet services such as FTP, Telnet, and the World Wide Web (WWW).

A more complicated filter set would be required to provide WAN access to a LAN-based server. See the next section, "[Possible modifications](#)," for ways to allow remote hosts to use services provided by servers on the LAN.

Possible modifications

You can modify the sample filter set Basic Firewall to allow incoming traffic using the examples below. These modifications are not intended to be combined. Each modification is to be the only one used with Basic Firewall.

The results of combining filter set modifications can be difficult to predict. It is recommended that you take special care if you are making more than one modification to the sample filter set.

Trusted host. To allow unlimited access by a trusted remote host with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: 255.255.255.255
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: 0

Trusted subnet. To allow unlimited access by a trusted remote subnet with subnet address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.0) and subnet mask e.f.g.h (corresponding to a numbered IP mask such as 255.255.255.0), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: a.b.c.d
- Source IP Address Mask: e.f.g.h
- Dest. IP Address: 0.0.0.0
- Dest. IP Address Mask: 0.0.0.0
- Protocol Type: 0

FTP sessions. To allow WAN-originated FTP sessions to a LAN-based FTP server with the IP address a.b.c.d (corresponding to a numbered IP address such as 163.176.8.243), insert the following input filter ahead of the current input filter 1:

- Enabled: Yes
- Forward: Yes
- Source IP Address: 0.0.0.0
- Source IP Address Mask: 0.0.0.0
- Dest. IP Address: a.b.c.d
- Dest. IP Address Mask: 255.255.255.255
- Protocol Type: TCP
- Source Port Comparison: No Compare
- Source Port ID: 0
- Dest. Port Comparison: Equal
- Dest. Port ID: 21

Note: A similar filter could be used to permit Telnet or WWW access. Set the Dest. Port ID to 23 for Telnet or to 80 for WWW.

Deleting a filter set does not delete the filters in that set. However, the filters in the deleted set are no longer in effect (unless they are part of another set). The deleted set will no longer appear in the answer profile or any connection profiles to which it was added.

Policy-based Routing using Filtersets

Previous firmware versions routed IP packets only by destination IP address. Netopia Firmware Version 8.4 now offers the ability to route IP packets using criteria other than the destination IP address. This is called *policy-based routing*. You are now able to route IP traffic based on the following:

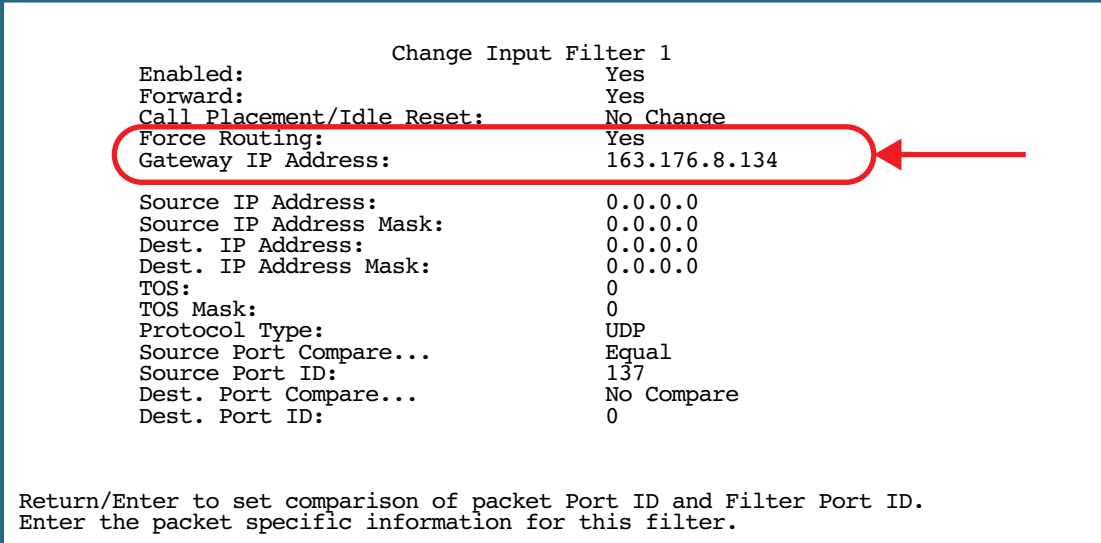
- source IP address
- source and/or destination protocol field
- source and/or destination port numbers
- TOS field

You specify the routing criteria and routing information by using IP filtersets to determine the forwarding action of a particular filter.

In previous firmware versions, a filter would either *pass* or *block* the specified traffic. Netopia Firmware Version 8.4 adds a third option, *force routing*. You specify a gateway IP address, and each packet matching the filter is routed according to that gateway address, rather than by means of the global routing table.

In addition, the TOS field has been added to the classifier list in a filter. This allows you to filter on TOS field settings in the IP packet, if you desire.

The new filterset screen appears as follows:



```

Change Input Filter 1
Enabled:                Yes
Forward:                Yes
Call Placement/Idle Reset: No Change
Force Routing:          Yes
Gateway IP Address:     163.176.8.134
Source IP Address:      0.0.0.0
Source IP Address Mask: 0.0.0.0
Dest. IP Address:       0.0.0.0
Dest. IP Address Mask: 0.0.0.0
TOS:                    0
TOS Mask:               0
Protocol Type:          UDP
Source Port Compare...  Equal
Source Port ID:         137
Dest. Port Compare...   No Compare
Dest. Port ID:          0

Return/Enter to set comparison of packet Port ID and Filter Port ID.
Enter the packet specific information for this filter.

```

To use the policy-based routing feature, you create a filter that forwards the traffic.

- Toggle **Forward** to **Yes**. This will display the Force Routing options.
- Toggle **Force Routing** to **Yes**.
- Enter the **Gateway IP Address** in standard dotted-quad notation to which the traffic should be forwarded.
- You can enter **Source** and **Destination IP Address(es)** and **Mask(s)**, **Protocol Type**, and **Source** and **Destination Port ID(s)** for the filter, if desired.

TOS field matching

Netopia Firmware Version 8.4 adds two additional new parameters to an IP filter: **TOS** and **TOS Mask**. Both fields accept values in the range 0 – 255.

Certain types of IP packets, such as voice or multimedia packets, are sensitive to latency introduced by the network. A delay-sensitive packet is one that has the low-latency bit set in the TOS field of the IP header. This means that if such packets are not received rapidly, the quality of service degrades. If you expect to route significant amounts of such traffic you can configure your router to route this type of traffic to a gateway other than your normal gateway using this feature.

The TOS field matching check is consistent with source and destination address matching.

Example: You want packets with the TOS low latency bit to go through VC 2 (via gateway 127.0.0.3) instead of your normal gateway. You would set up the filter as follows:

Add Input Filter	
Enabled:	Yes
Forward:	Yes
Call Placement/Idle Reset:	No Change
Force Routing:	Yes
Gateway IP Address:	127.0.0.3
Source IP Address:	0.0.0.0
Source IP Address Mask:	0.0.0.0
Dest. IP Address:	0.0.0.0
Dest. IP Address Mask:	0.0.0.0
TOS:	16
TOS Mask:	16
Protocol Type:	ANY

ADD THIS FILTER NOW CANCEL

Return/Enter to add this Filter to the Filter Set.
Enter the packet specific information for this filter.

Note:**Default Forwarding Filter**

If you create one or more filters that have a matching action of *forward*, then action on a packet matching *none* of the filters is to block any traffic.

Therefore, if the behavior you want is to force the routing of a certain type of packet and pass all others through the normal routing mechanism, you must configure one filter to match the first type of packet and apply Force Routing. A subsequent filter is required to match and forward all other packets.

Management IP traffic

If the Force Routing filter is applied to source IP addresses, it may inadvertently block communication with the router itself. You can avoid this by preceding the Force Routing filter with a filter that matches the destination IP address of the router itself.

Firewall Tutorial

General firewall terms

- Filter rule:** A filter set is comprised of individual filter rules.
- Filter set:** A grouping of individual filter rules.
- Firewall:** A component or set of components that restrict access between a protected network and the Internet, or between two networks.
- Host:** A workstation on the network.
- Packet:** Unit of communication on the Internet.
- Packet filter:** Packet filters allow or deny packets based on source or destination IP addresses, TCP or UDP ports, or the TCP ACK bit.
- Port:** A number that defines a particular type of service.

Basic IP packet components

All IP packets contain the same basic header information, as follows:

Source IP Address	163.176.132.18
Destination IP Address	163.176.4.27
Source Port	2541
Destination Port	80
Protocol	TCP
ACK Bit	Yes
DATA	User Data

This header information is what the packet filter uses to make filtering decisions. It is important to note that a packet filter does not look into the IP data stream (the User Data from above) to make filtering decisions.

Basic protocol types

- TCP:** Transmission Control Protocol. TCP provides reliable packet delivery and has a retransmission mechanism (so packets are not lost). RFC 793 is the specification for TCP.
 - UDP:** User Datagram Protocol. Unlike TCP, UDP does not guarantee reliable, sequenced packet delivery. If data does not reach its destination, UDP does not retransmit the data. RFC 768 is the specification for UDP.
- There are many more ports defined in the Assigned Addresses RFC. The table that follows shows some of these port assignments.

Example TCP/UDP Ports

TCP Port	Service	UDP Port	Service
20/21	FTP	161	SNMP
23	Telnet	69	TFTP
25	SMTP	387	AURP
80	WWW		
144	News		

Firewall design rules

There are two basic rules to firewall design:

- “What is not explicitly allowed is denied.”

and

- “What is not explicitly denied is allowed.”

The first rule is far more secure, and is the best approach to firewall design. It is far easier (and more secure) to allow in or out only certain services and deny anything else. If the other rule is used, you would have to figure out everything that you want to disallow, now and in the future.

Firewall Logic

Firewall design is a test of logic, and filter rule ordering is critical. If a packet is forwarded through a series of filter rules and then the packet matches a rule, the appropriate action is taken. The packet will not forward through the remainder of the filter rules.

For example, if you had the following filter set...

- Allow WWW access;
- Allow FTP access;
- Allow SMTP access;
- Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would forward through the first rule (WWW), go through the second rule (FTP), and match this rule; the packet is allowed through.

If you had this filter set for example....

- Allow WWW access;
- Allow FTP access;
- Deny FTP access;
- Deny all other packets.

and a packet goes through these rules destined for FTP, the packet would forward through the first filter rule (WWW), match the second rule (FTP), and the packet is allowed through. Even though the next rule is to deny all FTP traffic, the FTP packet will never make it to this rule.

Binary representation

It is easiest when doing filtering to convert the IP address and mask in question to binary. This will allow you to perform the logical AND to determine whether a packet matches a filter rule.

Logical AND function

When a packet is compared (in most cases) a logical AND function is performed. First the IP addresses and subnet masks are converted to binary and then combined with AND. The rules for the logical use of AND are as follows:

0 AND 0 = 0

0 AND 1 = 0

1 AND 0 = 0

1 AND 1 = 1

For example:

Filter rule:

Deny

IP: 163.176.1.15 BINARY: 10100011.10110000.00000001.00001111

Mask: 255.255.255.255 BINARY: 11111111.11111111.11111111.11111111

Incoming Packet:

IP 163.176.1.15 BINARY: 10100011.10110000.00000001.00001111

If you put the incoming packet and subnet mask together with AND, the result is:

10100011.10110000.00000001.00001111

which matches the IP address in the filter rule and the packet is denied.

Implied rules

With a given set of filter rules, there is an Implied rule that may or may not be shown to the user. The implied rule tells the filter set what to do with a packet that does not match any of the filter rules. An example of implied rules is as follows:

Implied	Meaning
Y+Y+Y=N	If all filter rules are YES, the implied rule is NO.
N+N+N=Y	If all filter rules are NO, the implied rule is YES.
Y+N+Y=N	If a mix of YES and NO filters, the implied rule is NO.

Established connections

The TCP header contains one bit called the ACK bit (or TCP Ack bit). This ACK bit appears only with TCP, not UDP. The ACK bit is part of the TCP mechanism that guarantees the delivery of data. The ACK bit is set whenever one side of a connection has received data from the other side. Only the first TCP packet will not have the ACK bit set; once the TCP connection is in place, the remainder of the TCP packets will have the ACK bit set.

The ACK bit is helpful for firewall design and reduces the number of potential filter rules. A filter rule could be created just allowing incoming TCP packets with the ACK bit set, since these packets had to be originated from the local network.

Example filter set screen

This is an example of the Netopia filter set screen:

Change Input Filter 1

Enabled:

Yes

Forward:

No

Source IP Address:

0.0.0.0

Source IP Address Mask:

0.0.0.0

Dest. IP Address:

0.0.0.0

Dest. IP Address Mask:

0.0.0.0

Protocol Type:

TCP

Source Port Compare...

No Compare

Source Port ID:

0

Dest. Port Compare...

Equal

Dest. Port ID:

2000

Established TCP Conns. Only:

No

Filter basics

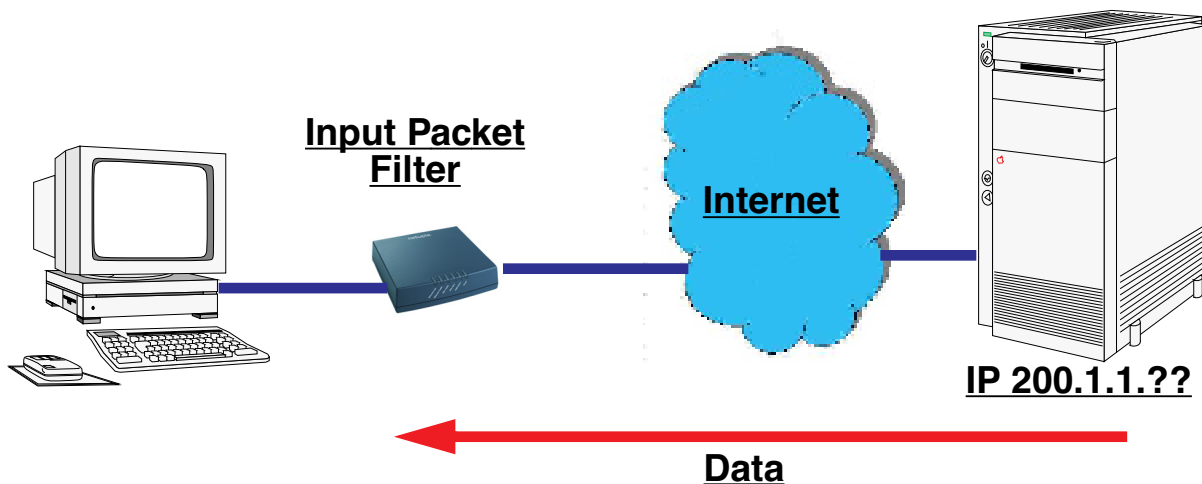
In the source or destination IP address fields, the IP address that is entered must be the network address of the subnet. A host address can be entered, but the applied subnet mask must be 32 bits (255.255.255.255).

The Netopia Firmware Version 8.4 has the ability to compare source and destination TCP or UDP ports. These options are as follows:

Item	What it means
No Compare	Does not compare TCP or UDP port
Not Equal To	Matches any port other than what is defined
Less Than	Anything less than the port defined

Less Than or Equal	Any port less than or equal to the port defined
Equal	Matches only the port defined
Greater Than or Equal	Matches the port or any port greater
Greater Than	Matches anything greater than the port defined

Example network



Example filters

Example 1

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.28

IP Address	Binary Representation	
200.1.1.28	00011100	(Source address in incoming IP packet)
AND		
255.255.255.128	10000000	(Perform the logical AND)

	00000000	(Logical AND result)
--	----------	----------------------

This incoming IP packet has a source IP address that matches the network address in the Source IP Address field (00000000) in the Netopia Firmware Version 8.4. This will *not* forward this packet.

Example 2

Filter Rule:	200.1.1.0	(Source IP Network Address)
	255.255.255.128	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184.

IP Address	Binary Representation	
200.1.1.184	10111000	(Source address in incoming IP packet)
AND		
255.255.255.128	10000000	(Perform the logical AND)
	10000000	(Logical AND result)

This incoming IP packet (10000000) has a source IP address that does not match the network address in the Source IP Address field (00000000) in the Netopia Firmware Version 8.4. This rule *will* forward this packet because the packet does not match.

Example 3

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.184.

IP Address	Binary Representation	
200.1.1.184	10111000	(Source address in incoming IP packet)
AND		
255.255.255.240	11110000	(Perform the logical AND)

	10110000	(Logical AND result)
--	----------	----------------------

Since the Source IP Network Address in the Router is 01100000, and the source IP address after the logical AND is 1011000, this rule does *not* match and this packet will be forwarded.

Example 4

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.240	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.104.

IP Address	Binary Representation	
200.1.1.104	01101000	(Source address in incoming IP packet)
AND		
255.255.255.240	11110000	(Perform the logical AND)
	01100000	(Logical AND result)

Since the Source IP Network Address in the Router is 01100000, and the source IP address after the logical AND is 01100000, this rule *does* match and this packet will *not* be forwarded.

Example 5

Filter Rule:	200.1.1.96	(Source IP Network Address)
	255.255.255.255	(Source IP Mask)
	Forward = No	(What happens on match)

Incoming packet has the source address of 200.1.1.96.

IP Address	Binary Representation	
200.1.1.96	01100000	(Source address in incoming IP packet)
AND		
255.255.255.255	11111111	(Perform the logical AND)

	01100000	(Logical AND result)
--	----------	----------------------

Since the Source IP Network Address in the Router is 01100000, and the source IP address after the logical AND is 01100000, this rule *does* match and this packet will *not* be forwarded. This rule masks off a *single* IP address.

Configuration Management

Netopia Firmware Version 8.4 offers a Configuration Management feature. Configuration Management provides a way to store several gateway configurations in a single device for use at different times.

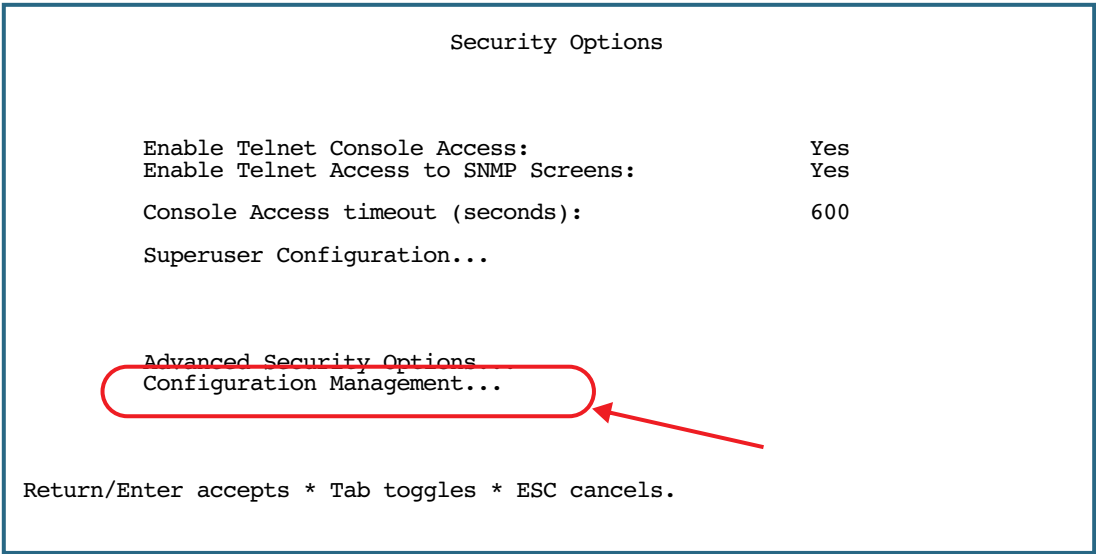
You can store up to three configurations in the gateway’s memory in addition to the currently running configuration. The current configuration is the one currently booted from and is updated whenever there is a change to the gateway (logged events, parameter changes).

Other configurations are stored along with the current configuration. Whenever you choose, you can reboot into one of these configurations (the copy of which becomes the current configuration).

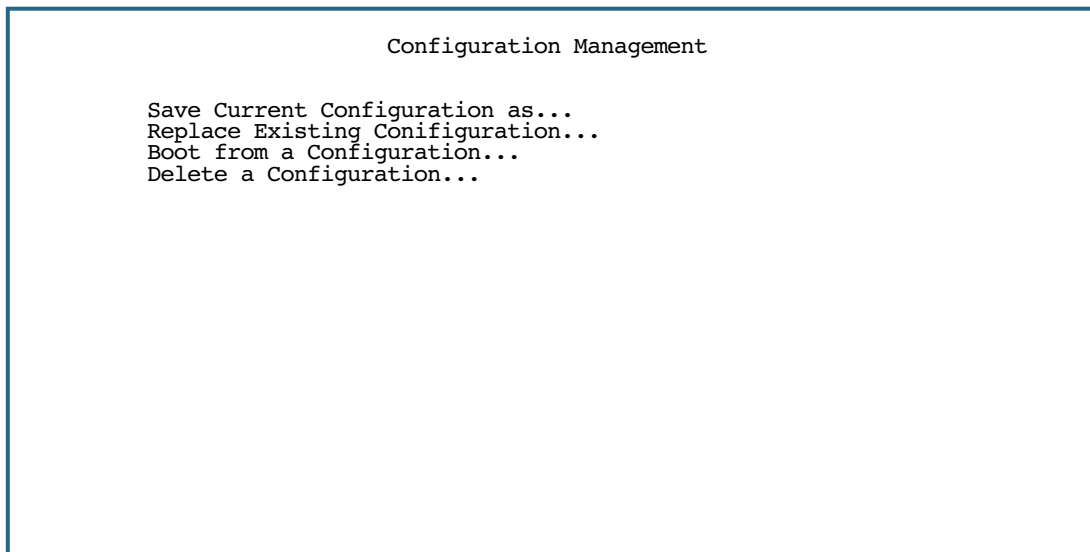
You name the saved configurations, giving you a reference for identifying each one. The naming operation occurs when you decide to save a configuration or when downloading a configuration via TFTP.

The configurations that are saved will persist across a Factory Default (soft or NMI). The gateway will reboot with a Factory Defaulted configuration, as usual, but the saved configurations are still available for use.

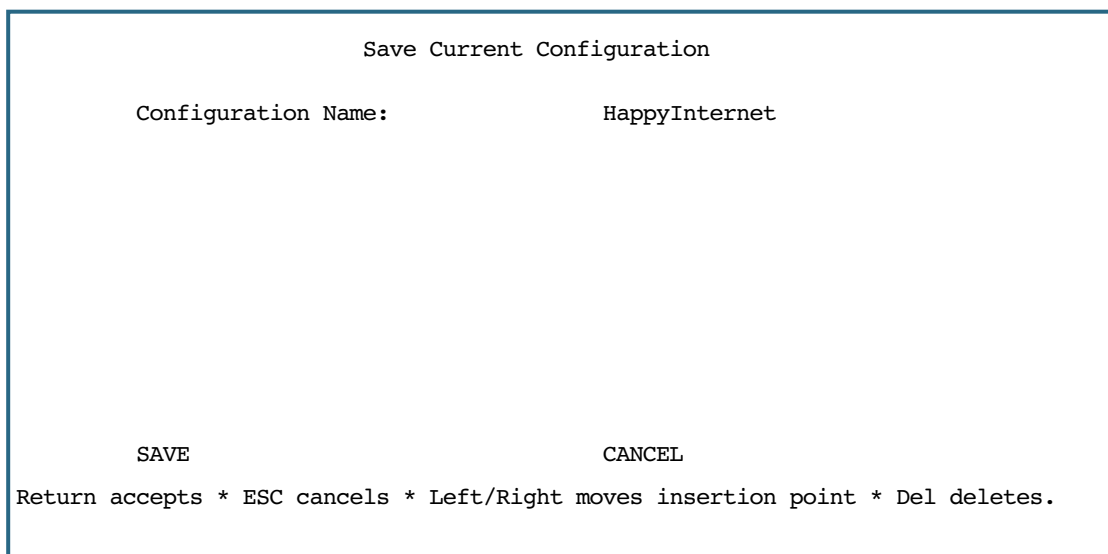
You save your configurations in the Configuration Management screen in the Security menus.



Select **Configuration Management**, and press Return. The Configuration Management screen appears.

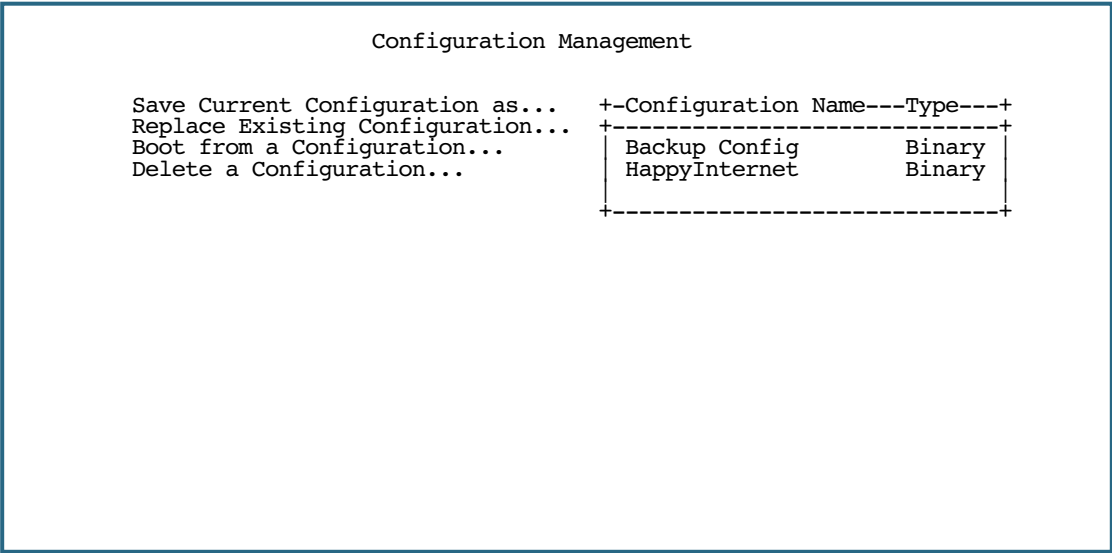


Select **Save Current Configuration as**, and press Return. The Save Current Configuration screen appears.



Enter a descriptive name for your current configuration, select **SAVE**, and press Return. Your configuration will be saved to the flash memory, and you will be returned to the Configuration Management screen.

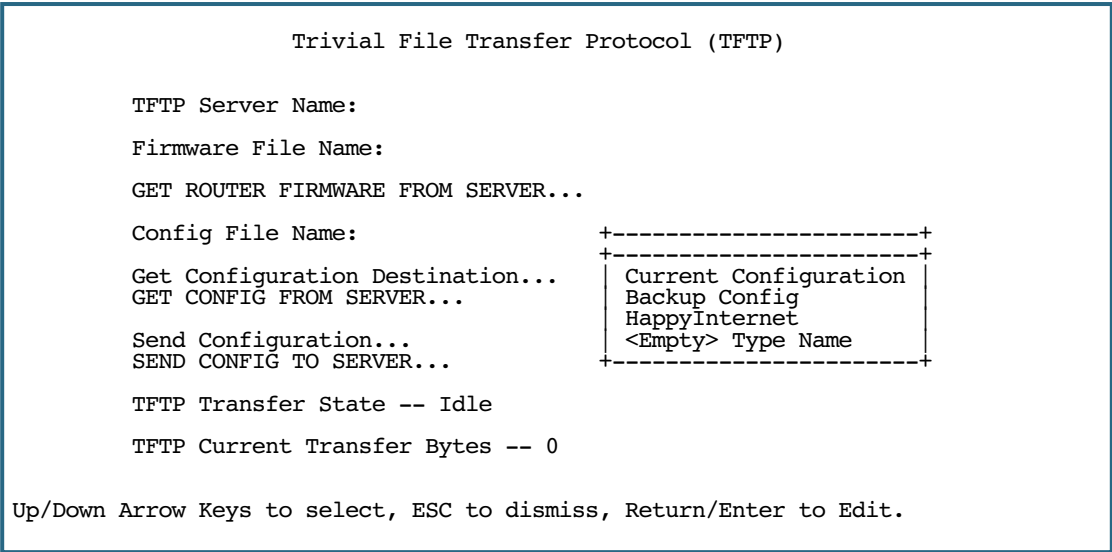
If you choose to run one of your stored configurations, you can select it from a pop-up menu. If you select **Boot from a Configuration** and select a different one, you can reboot the gateway with your selected configuration.



A warning screen will ask you to confirm your choice.

TFTP

You can also send or receive your stored configuration files via TFTP. You select the stored configuration files from pull-down menus in the TFTP File Transfer screen in the Utilities & Diagnostics menu, as shown.



Chapter 10

Utilities and Diagnostics

A number of utilities and tests are available for system diagnostic and control purposes.

This section covers the following topics:

- [“Ping” on page 10-2](#)
- [“Trace Route” on page 10-4](#)
- [“Telnet Client” on page 10-5](#)
- [“Factory Defaults” on page 10-6](#)
- [“Transferring Configuration and Firmware Files with TFTP” on page 10-6](#)
- [“Restarting the System” on page 10-8](#)

Note: These utilities and tests are accessible only through the Telnet-based management screens. See the *Getting Started Guide* chapter, “Telnet-Based Management,” for information on accessing the Telnet-based management screens.

You access the Utilities & Diagnostics screens from the Main Menu.

Utilities & Diagnostics...

Ping...
Trace Route...
Telnet...

Disconnect Telnet Console Session...
Trivial File Transfer Protocol (TFTP)...

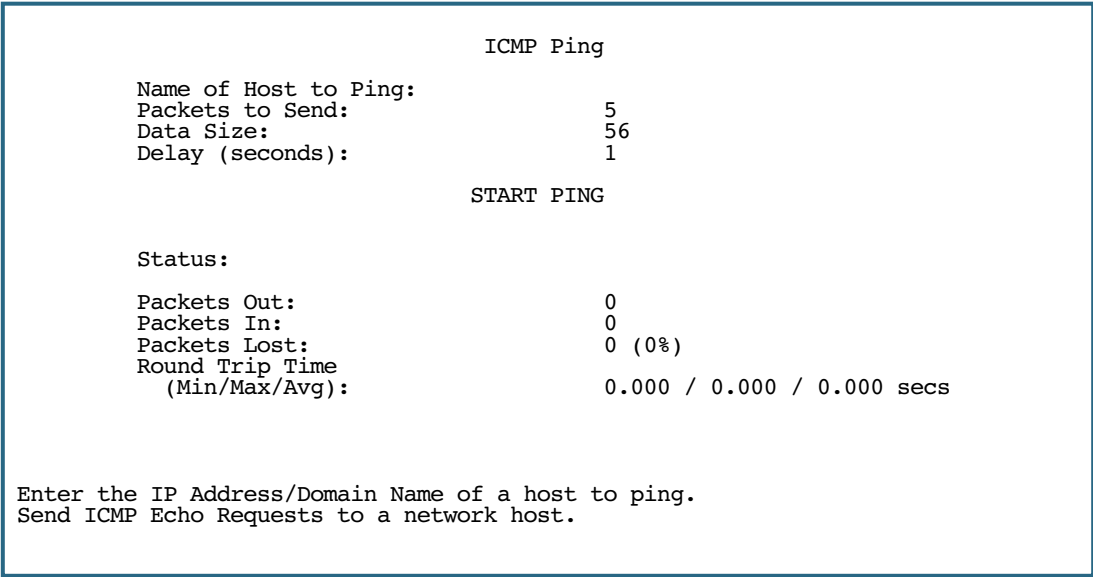
Restart System... Revert to Factory Defaults...

Ping

The Netopia Firmware Version 8.4 includes a standard Ping test utility. A Ping test generates IP packets destined for a particular (Ping-capable) IP host. Each time the target host receives a Ping packet, it returns a packet to the original sender.

Ping allows you to see whether a particular IP destination is reachable from the Router. You can also ascertain the quality and reliability of the connection to the desired destination by studying the Ping test's statistics.

In the Utilities & Diagnostic screen, select **Ping** and press Return. The ICMP Ping screen appears.



To configure and initiate a Ping test, follow these steps:

1. Select **Name of Host to Ping** and enter the destination domain name or IP address.
2. Select **Packets to Send** to change the default setting. This is the total number of packets to be sent during the Ping test. The default setting is adequate in most cases, but you can change it to any value from 1 to 4,294,967,295.
3. Select **Data Size** to change the default setting. This is the size, in bytes, of each Ping packet sent. The default setting is adequate in most cases, but you can change it to any value from 0 (only header data) to 1664.
4. Select **Delay (seconds)** to change the default setting. The delay, in seconds, determines the time between Ping packets sent. The default setting is adequate in most cases, but you can change it to any value from 0 to 4,294,967. A delay of 0 seconds forces packets to be sent immediately, one after another.
5. Select **START PING** and press Return to begin the Ping test. While the test is running, the **START PING** item becomes **STOP PING**. To manually stop the Ping test, select **STOP PING** and press Return or Escape.

While the Ping test is running and when it is over, a status field and a number of statistical items are active on the screen. These are described below.

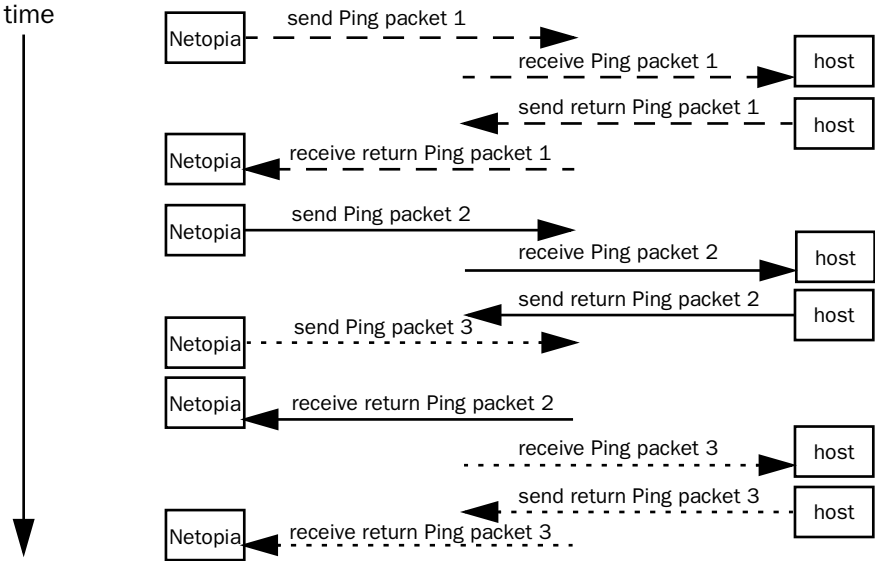
Status: The current status of the Ping test. This item can display the status messages shown in the table below:

Message	Description
Resolving host name	Finding the IP address for the domain name-style address
Can't resolve host name	IP address can't be found for the domain name-style address
Pinging	Ping test is in progress
Complete	Ping test was completed
Cancelled by user	Ping test was cancelled manually
Destination unreachable from w.x.y.z	Ping test was able to reach the gateway with IP address w.x.y.z, which reported that the test could not reach the final destination
Couldn't allocate packet buffer	Couldn't proceed with Ping test; try again or reset system
Couldn't open ICMP port	Couldn't proceed with Ping test; try again or reset system

Packets Out: The number of packets sent by the Ping test.

Packets In: The number of return packets received from the target host. To be considered on time, return packets are expected back before the next packet in the sequence of Ping packets is sent. A count of the number of late packets appears in parentheses to the right of the **Packets In** count.

In the example that follows, a Router is sending Ping packets to another host, which responds with return Ping packets. Note that the second return Ping packet is considered to be late because it is not received by the Router before the third Ping packet is sent. The first and third return Ping packets are on time.



Packets Lost: The number of packets unaccounted for, shown in total and as a percentage of total packets sent. This statistic may be updated during the Ping test, and may not be accurate until after the test is over. However, if an escalating one-to-one correspondence is seen between **Packets Out** and **Packets Lost**, and **Packets In** is noticeably lagging behind **Packets Out**, the destination is probably unreachable. In this case, use **STOP PING**.

Round Trip Time (Min/Max/Avg): Statistics showing the minimum, maximum, and average number of seconds elapsing between the time each Ping packet was sent and the time its corresponding return Ping packet was received.

The time-to-live (TTL) value for each Ping packet sent by the Router is 255, the maximum allowed. The TTL value defines the number of IP gateways that the packet can traverse. Ping packets that reach their TTL value are dropped, and a “destination unreachable” notification is returned to the sender (see the table on the previous page). This ensures that no infinite routing loops occur. The TTL value can be set and retrieved using the SNMP MIB-II ip group’s ipDefaultTTL object.

Trace Route

You can count the number of gateways between your Netopia Router and a given destination with the Trace Route utility.

In the Statistics & Diagnostics screen, select **Trace Route** and press Return. The Trace Route screen appears.

Trace Route

Host Name or IP Address:

Maximum Hops:30

Timeout (seconds):5

Use Reverse DNS:Yes

START TRACE ROUTE

Enter the IP Address/Domain Name of a host.
Trace route to a network host.

To trace a route, follow these steps:

1. Select **Host Name or IP Address** and enter the name or address of the destination you want to trace.
2. Select **Maximum Hops** to set the maximum number of gateways to count between the Netopia Router and the destination gateway, up to the maximum of 64. The default is 30 hops.
3. Select **Timeout (seconds)** to set when the trace will timeout for each hop, up to 10 seconds. The default is 3 seconds.

4. Select **Use Reverse DNS** to learn the names of the gateways between the Netopia Router and the destination gateway. The default is Yes.
5. Select **START TRACE ROUTE** and press Return. A scrolling screen will appear that lists the destination, number of hops, IP addresses of each hop, and DNS names, if selected.
6. Cancel the trace by pressing Escape. Return to the Trace Route screen by pressing Escape twice.

Telnet Client

The Telnet client mode replaces the normal menu mode. Telnet sessions can be cascaded, that is, you can initiate a Telnet client session when using a Telnet console session. To activate the Telnet client, select **Telnet** from the Utilities & Diagnostics menu.

The Telnet client screen appears.

Telnet

Host Name or IP Address:

Control Character to Suspend: Q

START A TELNET SESSION

Resume Suspended Session...

Terminate Suspended Session...

- Enter the host name or the IP address in dotted decimal format of the machine you want to Telnet into and press Return.
- Either accept the default control character “Q” used to suspend the Telnet session, or type a different one.
- **START A TELNET SESSION** becomes highlighted.
- Press Return and the Telnet session will be initiated.
- To suspend the session, press Control-Q or whatever other control character you specified.
- To go back to your Telnet session, select **Resume Suspended Session**. Select a session from the pop-up menu and press Return.
- To end a suspended session, select **Terminate Suspended Session**. Select a session from the pop-up menu and press Return.

Factory Defaults

You can reset the Router to its factory default settings. In the Utilities & Diagnostics screen, select **Revert to Factory Defaults** and press Return. Select **CONTINUE** in the dialog box and press Return. The Router will reboot and its settings will return to the factory defaults, deleting your configurations.

In an emergency, you can also use the Reset switch to return the gateway to its factory default settings. Call Netopia Technical Support for instructions on using the Reset switch.

Note: Reset to factory defaults with caution. You will need to reconfigure all of your settings in the gateway.

If you lose your password and are unable to access the Telnet screens, you can manually reset the gateway in an emergency. See [Appendix A, “Troubleshooting.”](#)

Transferring Configuration and Firmware Files with TFTP

Trivial File Transfer Protocol (TFTP) is a method of transferring data over an IP network. TFTP is a client-server application, with the gateway as the client. To use the Router as a TFTP client, a TFTP server must be available. Netopia, Inc., has a public access TFTP server on the Internet where you can obtain the latest firmware versions.

To use TFTP, select **Trivial File Transfer Protocol (TFTP)** in the Statistics & Diagnostics screen and press Return. The Trivial File Transfer Protocol (TFTP) screen appears.

```
Trivial File Transfer Protocol (TFTP)

TFTP Server Name:

Firmware File Name:      /Users/njbill/Desktop/n808.bin
GET ROUTER FIRMWARE FROM SERVER...

Config File Name:

Get Configuration Destination...  Current Configuration
GET CONFIG FROM SERVER...

Send Configuration...           Current Configuration
SEND CONFIG TO SERVER...

TFTP Transfer State -- Idle

TFTP Current Transfer Bytes -- 0
```

The sections below describe how to update the Router's firmware and how to download and upload configuration files.

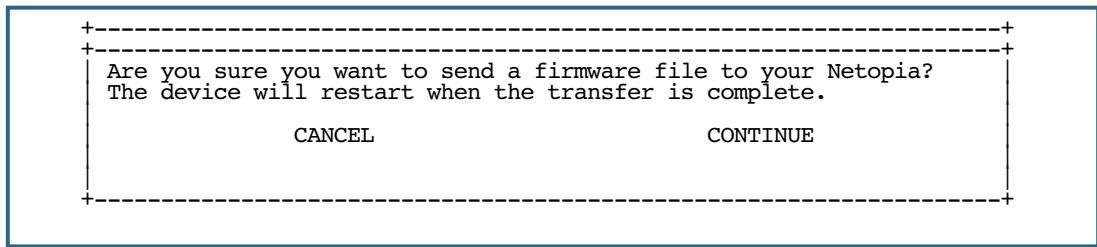
Updating firmware

Firmware updates may be available periodically from Netopia or from a site maintained by your organization's network administrator.

The Router ships with an embedded operating system referred to as firmware. The firmware governs how the device communicates with your network and the WAN or remote site. Firmware updates are periodically posted on the Netopia website.

To update the gateway's firmware, follow these steps:

- Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.
- Select **Firmware File Name** and enter the name of the file you will download. The name of the file is available from the site where the server is located. You may need to enter a file path along with the file name (for example, bigroot/config/myfile).
- Select **GET GATEWAY FIRMWARE FROM SERVER** and press Return. You will see the following dialog box:



- Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file. The system will reset at the end of the file transfer to put the new firmware into effect. While the system resets, the LEDs will blink on and off.

Caution!

- Be sure the firmware update you load onto your gateway is the correct version for your particular model. Some models do not support all firmware versions. Loading an incorrect firmware version can permanently damage the unit.
- Do not manually power down or reset the Router while it is automatically resetting or it could be damaged.
- If you choose to download the firmware, the **TFTP Transfer State** item will change from **Idle** to **Reading Firmware**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Downloading configuration files

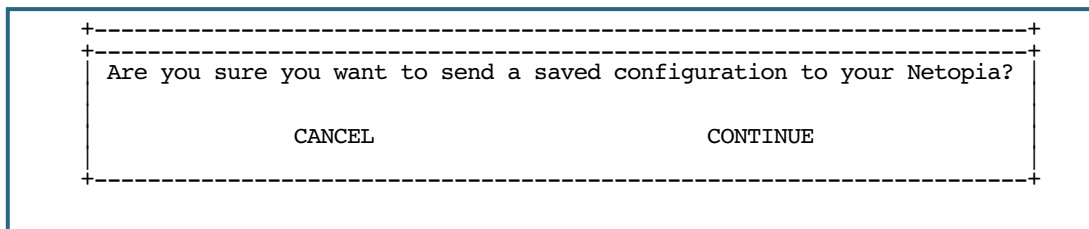
The Router can be configured by downloading a configuration file using TFTP. Once downloaded, the file reconfigures all of the gateway's parameters.

To download a configuration file, follow these steps:

- Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.

10-8 Firmware User Guide

- Select **Config File Name** and enter the name of the file you will download. The name of the file is available from the site where the server is located. You may need to enter a file path along with the file name (for example, bigroot/config/myfile).
- Select **GET CONFIG FROM SERVER** and press Return. You will see the following dialog box:



- Select **CANCEL** to exit without downloading the file, or select **CONTINUE** to download the file. The system will reset at the end of the file transfer to put the new configuration into effect.
- If you choose to download the configuration file, the **TFTP Transfer State** item will change from **Idle** to **Reading Config**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Uploading configuration files

Using TFTP, you can send a file containing a snapshot of the gateway's current configuration to a TFTP server. The file can then be downloaded by a different Router unit to configure its parameters (see [“Downloading configuration files” on page 10-7](#)). This is useful for configuring a number of gateways with identical parameters or just for creating configuration backup files.

Uploading a file can also be useful for troubleshooting purposes. The uploaded configuration file can be tested on a different Router unit by Netopia or your network administrator.

To upload a configuration file, follow these steps:

1. Select **TFTP Server Name** and enter the server name or IP address of the TFTP server you will use. The server name or IP address is available from the site where the server is located.
2. Select **Config File Name** and enter a name for the file you will upload. The file will appear with the name you choose on the TFTP server. You may need to enter a file path along with the file name (for example, Mypc/Netopia/myfile).
3. Select **SEND CONFIG TO SERVER** and press Return. Netopia will begin to transfer the file.
4. The **TFTP Transfer State** item will change from **Idle** to **Writing Config**. The **TFTP Current Transfer Bytes** item will reflect the number of bytes transferred.

Restarting the System

You can restart the system by selecting the **Restart System** item in the Utilities & Diagnostics screen.

You must restart the system whenever you reconfigure the Router and want the new parameter values to take effect. Under certain circumstances, restarting the system may also clear up system or network malfunctions. Some configuration processes automatically restart the system to apply the changes you have made.

Appendix A

Troubleshooting

This appendix is intended to help you troubleshoot problems you may encounter while setting up and using Netopia Firmware Version 8.4. It also includes information on how to contact Netopia Technical Support.

Important information on these problems can be found in the event histories kept by the Router. These event histories can be accessed in the Statistics & Logs screen.

This section covers the following topics:

- [“Configuration Problems” on page A-1](#)
- [“How to Reset the Router to Factory Defaults” on page A-3](#)
- [“Power Outages” on page A-3](#)
- [“Technical Support” on page A-3](#)

Configuration Problems

If you encounter problems during your initial configuration process, review the following suggestions before calling for technical support. There are four zones to consider when troubleshooting initial configuration:

1. The computer's connection to the gateway
2. The gateway's connection to the telecommunication line(s)
3. The telecommunication line's connection to your ISP
4. The ISP's connection to the Internet

If the connection from the computer to the gateway was not successful, verify that the following conditions are in effect:

- The Router is turned on.
- An Ethernet cable connects your PC's Ethernet card or built-in Ethernet port to the Router.
- Telnet is available on your PC or Macintosh. (On a PC, it must be specified in your system path. You can usually find the application as “c:\windows\telnet.exe”.)
- Your PC or Macintosh is properly configured for TCP/IP.
- Your PC or Macintosh has an IP address.
- Your PC or Macintosh has a subnet mask that matches or is compatible with the Router's subnet mask.

Note: If you are attempting to modify the IP address or subnet mask from a previous, successful configuration attempt, you will need to clear the IP address or reset your Router to the factory default before reinitiating the configuration process. For further information on resetting your Router to factory default, see [“How to Reset the Router to Factory Defaults” on page A-3](#).

Network problems

Problems communicating with remote IP hosts

- Verify the accuracy of the default gateway’s IP address (entered in the IP Setup or Easy Setup screen).
- Use the Netopia Firmware Version 8.4’s Ping utility, in the Utilities & Diagnostics screen, and try to Ping local and remote hosts. See [“Ping” on page 10-2](#) for instructions on how to use the Ping utility. If you can successfully Ping hosts using their IP addresses but not their domain names (198.34.7.1 but not garcia.netopia.com, for example), verify that the DNS server’s IP address is correct and that it is reachable from the Router (use Ping).
- If you are using filters, check that your filter sets are not blocking the type of connections you are trying to make.

Local routing problems

- Observe the Ethernet LEDs to see if data traffic flow appears to be normal.
- Check the WAN statistics and LAN statistics screens to see more specific information on data traffic flow and address serving. See [“Statistics & Logs” on page 8-4](#) for more information.

How to Reset the Router to Factory Defaults

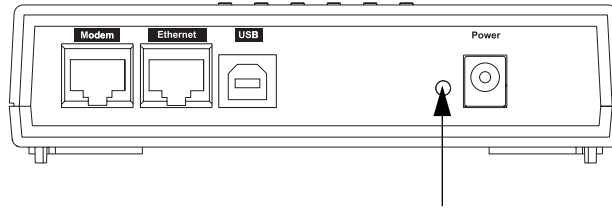
Lose your password? This section shows how to reset the Netopia Router so that you can access the configuration screens once again.

Note: Keep in mind that all of your settings will need to be reconfigured.

If you don't have a password, the only way to access the Netopia Router is the following:

1. Referring to the diagram below, find the round Reset Switch opening.

Example Netopia Router back panel



Factory Reset Switch: Push to clear all settings

2. Carefully insert the point of a pen or an unwound paperclip into the opening.
3. Press this switch.

This will reset the unit to factory defaults and you will now be able to reprogram your Router.

Power Outages

If you suspect that power was restored after a power outage and the Router is connected to a remote site, you may need to switch the Router off and then back on again. After temporary power outages, a connection that still seems to be up may actually be disconnected. Rebooting the gateway should reestablish the connection.

Technical Support

Netopia, Inc. is committed to providing its customers with reliable products and documentation, backed by excellent technical support.

Before contacting Netopia

Look in this guide for a solution to your problem. You may find a solution in this troubleshooting appendix or in other sections. Check the index for a reference to the topic of concern. If you cannot find a solution, complete the environment profile below before contacting Netopia Technical Support.

Environment profile

- Locate the Router's model number, product serial number, and firmware version. The serial number is on the bottom of the gateway, along with the model number. The firmware version appears in the Netopia Netopia Router's Main Menu screen.

Model number:

Serial number:

Firmware version:

- What kind of local network(s) do you have, with how many devices?

Ethernet

TCP/IP

How to reach us

We can help you with your problem more effectively if you have completed the environment profile in the previous section. If you contact us by telephone, please be ready to supply Netopia Technical Support with the information you used to configure the Router. Also, please be at the site of the problem and prepared to reproduce it and to try some troubleshooting steps.

When you are prepared, contact Netopia Technical Support by e-mail, telephone, fax, or post:

Internet: ask_netopia@netopia.com (for technical support)

info@netopia.com (for general information)

Phone: 1 510-597-5400

Fax: 1 510-420-7601

Netopia, Inc.

Customer Services

6001 Shellmound Street

Emeryville, California 94608

USA

Online product information

Product information can be found in the following:

Netopia World Wide Web server via <http://www.netopia.com>

Internet via anonymous FTP to <ftp.netopia.com/pub>

Appendix B

Understanding IP Addressing

This appendix is a brief general introduction to IP addressing. A basic understanding of IP will help you in configuring the Netopia Firmware Version 8.4 and using some of its powerful features, such as static routes and packet filtering.

This section covers the following topics:

- [“What is IP?” on page B-1](#)
- [“About IP Addressing” on page B-1](#)
- [“Distributing IP Addresses” on page B-5](#)
- [“Nested IP Subnets” on page B-11](#)
- [“Broadcasts” on page B-14](#)

What is IP?

All networks use protocols to establish common standards for communication. One widely used network protocol is the Internet Protocol, also known as IP. Like many other protocols, IP uses packets, or formatted chunks of data, to communicate. In packets, a header is part of the envelope information that surrounds the actual data being transmitted. In e-mail, a header is usually the address and routing information found at the top of messages.

Note: This guide uses the term “IP” in a very general and inclusive way to identify all of the following:

- Networks that use the Internet Protocol, along with accompanying protocols such as TCP, UDP, and ICMP
 - Packets that include an IP header within their structure
 - Devices that send IP packets
-

About IP Addressing

Every networking protocol uses some form of addressing in order to ensure that packets are delivered correctly. In IP, individual network devices that are initial sources and final destinations of packets are usually called hosts instead of nodes, but the two terms are interchangeable. Each host on an IP network must have a unique IP address. An IP address, also called an Internet address, is a 32-bit number usually expressed as four decimal numbers separated by periods. Each decimal number in an IP address represents a 1-byte (8-bit) binary number. Thus, values for each of the four numbers range from 00000000 to 11111111 in binary notation, or from 0 to 255 in decimal notation. The expression 192.168.1.1 is a typical example of an IP address.

IP addresses indicate both the identity of the network and the identity of the individual host on the network. The number of bits used for the network number and the number of bits used for the host number can vary, as long as certain rules are followed. The local network manager assigns IP host numbers to individual machines.

IP addresses are maintained and assigned by the InterNIC, a quasi-governmental organization now increasingly under the auspices of private industry.

Note: It's very common for an organization to obtain an IP address from a third party, usually an Internet service provider (ISP). ISPs usually issue an IP address when they are contracted to provide Internet access services.

The InterNIC (the NIC stands for Network Information Center) divides IP addresses into several classes. Classes A, B, and C are assigned to organizations that request addresses. In Class A networks, the first byte of an IP address is reserved for the network portion of the address. Class B networks reserve the first two bytes of an IP address for the network address. Class C networks reserve the first three bytes of an IP address for the network address. In all cases, a network manager can decide to use subnetting to assign even more bits to the network portion of the IP address, but never less than the class requires. The following section gives more information on subnetting.

Class A networks have a small number of possible network numbers, but a large number of possible host numbers. Conversely, Class C networks have a small number of possible host numbers, but a large number of possible network numbers. Thus, the InterNIC assigns Class A addresses to large organizations that have very large numbers of IP hosts, while smaller organizations, with fewer hosts, get Class B or Class C addresses. You can tell the various classes apart by the value of the first (or high-order) byte. Class A networks use values from 1 to 127, Class B networks use values from 128 to 191, and Class C networks use values from 192 to 223. The following table summarizes some of the differences between Class A, B, and C networks.

Class	First byte	Number of networks possible per class	Number of hosts possible per network	Format of address (without subnetting)	Example
A	1–127	127	16,777,214	net.host.host.host	97.3.14.250
B	128–191	16,384	65,534	net.net.host.host	140.100.10.11
C	192–223	2,097,152	254	net.net.net.host	197.204.13.7

Subnets and subnet masks

Often an entire organization is assigned only one IP network number. If the organization has several IP networks connected together with IP gateways, the network manager can use subnetting to distinguish between these networks, even though they all use the same network number. Each physical network becomes a subnet with a unique subnet number.

Subnet numbers appear within IP addresses, along with network numbers and host numbers. Since an IP address is always 32 bits long, using subnet numbers means either the network number or the host numbers must use fewer bits in order to leave room for the subnet numbers. Since the InterNIC assigns the network number proper, it should not change, so the subnet numbers must be created out of bits that would otherwise be part of the host numbers.

Subnet masks

To create subnets, the network manager must define a subnet mask, a 32-bit number that indicates which bits in an IP address are used for network and subnetwork addresses and which are used for host addresses. One subnet mask should apply to all IP networks that are physically connected together and share a single assigned network number. Subnet masks are often written in decimal notation like IP addresses, but they are most easily understood in binary notation. When a subnet mask is written in binary notation, each numeral 1 indicates that the corresponding bit in the IP address is part of the network or subnet address. Each 0 indicates that the corresponding bit is part of the host address. The following table shows the proper subnet masks to use for each class of network when no subnets are required.

Class	Subnet mask for a network with no subnets
A	Binary: 11111111.00000000.00000000.00000000 Decimal: 255.0.0.0
B	Binary: 11111111.11111111.00000000.00000000 Decimal: 255.255.0.0
C	Binary: 11111111.11111111.11111111.00000000 Decimal: 255.255.255.0

To know whether subnets are being used or not, you must know what subnet mask is being used—you cannot determine this information simply from an IP address. Subnet mask information is configured as part of the process of setting up IP gateways and gateways such as the Router.

Note: If you receive a routed account from an ISP, there must be a mask associated with your network IP address. By using the IP address with the mask you can discover exactly how many IP host addresses you actually have.

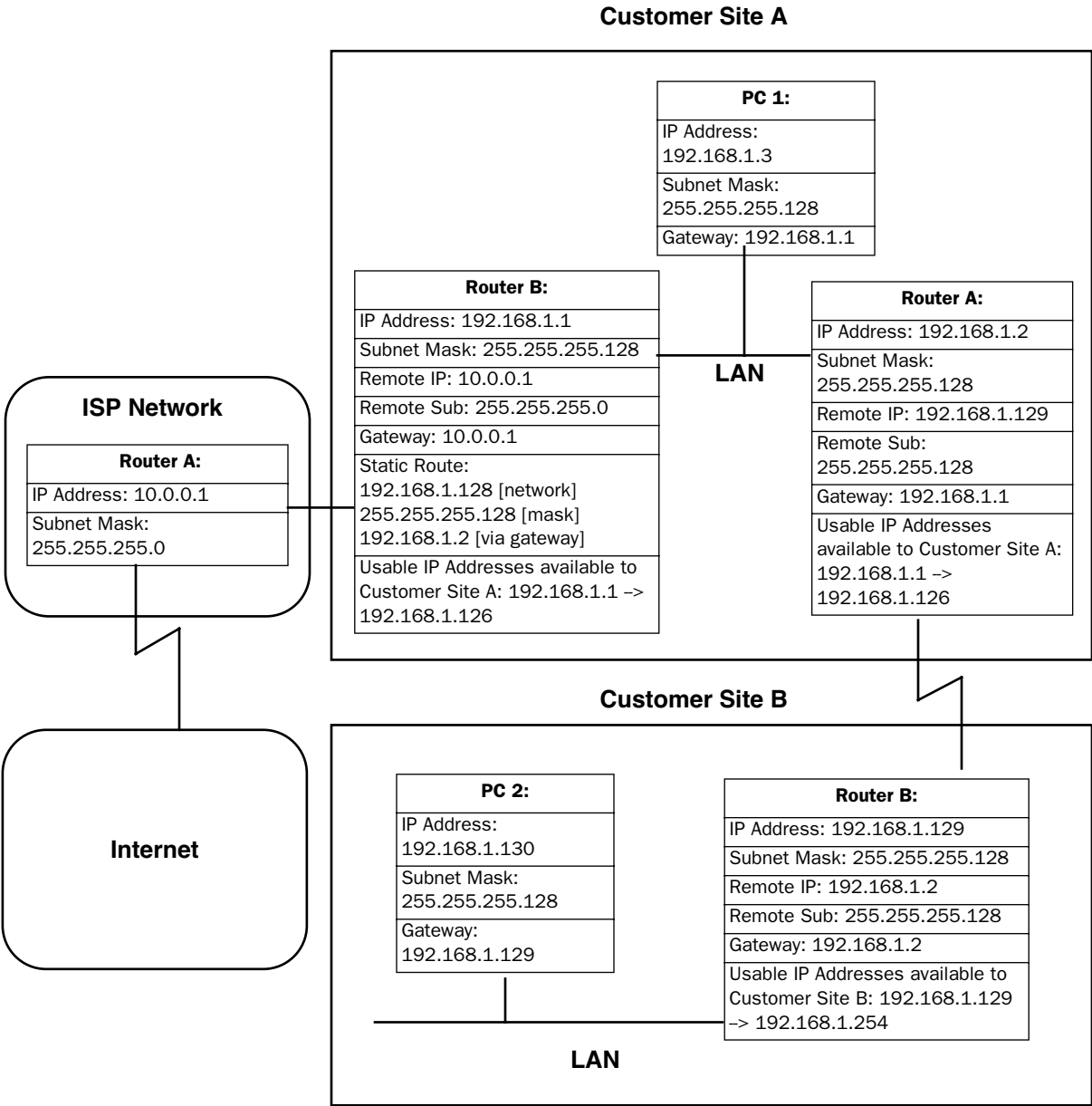
To configure subnets properly, you must also be able to convert between binary notation and decimal notation.

Example: Using subnets on a Class C IP internet

When setting up IP routing with a Class A address, or even with multiple Class C addresses, subnetting is fairly straightforward. Subnetting a single Class C address between two networks, however, is more complex. This section describes the general procedures for subnetting a single Class C network between two Netopia gateways so that each can have Internet access.

Network configuration

Below is a diagram of a simple network configuration. The ISP is providing a Class C address to the customer site, and both networks A and B want to gain Internet access through this address. Router B connects to Router A and is provided Internet access through Routers A and B.



Background

The IP addresses and routing configurations for the devices shown in the diagram are outlined below. In addition, each individual field and its meaning are described.

The IP Address and Subnet Mask fields define the IP address and subnet mask of the device's Ethernet connection to the network while the Remote IP and Remote Sub fields describe the IP address and subnet mask of the remote gateway. This information is entered in the connection profile of the Router.

The Router field describes the gateway or workstation's default gateway, or where they will send their packets if the appropriate route is not known. The Static Route field, which is only shown on Router B, tells Router B what path to take to get to the network defined by Router B. Finally, the Usable IP Address field shows the range of IP addresses available to the hosts of that network.

Note that the IP addresses given in this section are for example purposes only. Do not use these addresses when configuring your network.

With this configuration, both Customer Site A and B can gain Internet access through Routers A and B, with no reconfiguration of the ISP's equipment. The most important item in this configuration is the static route defined on Router B. This tells Router B what path to take to get to the network defined by Router B. Without this information, Customer Site B will be able to access Customer Site A, but not the Internet.

If it is not possible to define a static route on Router B, RIP could be enabled to serve the same purpose. To use RIP instead of a static route, enable Transmit RIP on Router A and Transmit and Receive RIP on Router B. This will allow the route from Customer Site B to propagate on Router B and Customer Site A.

Example: Working with a Class C subnet

Suppose that your organization has a site with only 10 hosts and no plans to add any new hosts. You don't need a full Class C address for this site. Many ISPs offer Internet access with only a portion of a full Internet address.

For example, you might obtain the Class C address 199.14.17.48, with the mask 255.255.255.240. From the previous example, you can see that this gives you 14 host addresses to distribute to the hosts at your site. In effect, your existing network of 10 hosts is a subnet of the ISP's network. Since the Class C address has already been reduced to subnets, you cannot further subnet your network without the risk of creating network routing problems (since you must use the mask issued by the ISP). This, however, is not a problematic limitation for your small network.

The advantages of this situation are the greater ease and lower cost of obtaining a subnet rather than a full Class C address from an ISP.

Distributing IP Addresses

To set up a connection to the Internet, you may have obtained a block of IP host addresses from an ISP. When configuring the Router, you gave one of those addresses to its Ethernet port, leaving a number of addresses to distribute to computers on your network.

There are two schemes for distributing the remaining IP addresses:

- Manually give each computer an address
- Let the Router automatically distribute the addresses

These two methods are not mutually exclusive; you can manually issue some of the addresses while the rest are distributed by the Router. Using the gateway in this way allows it to function as an address server.

One reason to use the Router as an address server is that it takes less time than manually distributing the addresses. This is particularly true if you have many addresses to distribute. You need to enter information only once, rather than having to enter it on each host separately. This also reduces the potential for misconfiguring hosts.

Another reason to use the Router as an address server is that it will distribute addresses only to hosts that need to use them.

All Routers come with an integrated Dynamic Host Control Protocol (DHCP) server. Some gateways also come with a Macintosh Internet Protocol (MacIP) server. These servers provide a means of distributing IP addresses to either a Mac or PC workstation as needed.

When setting up the DHCP or MacIP servers in the Router, it is necessary to understand how workstations lease, renew, and release their IP addresses. This information is helpful in determining dynamic address allocation for a network.

The term “lease” describes the action of a workstation requesting and using an IP address. The address is dynamic and can be returned to the address pool at a later time.

The term “renew” refers to what the workstations do to keep their leased IP address. At certain intervals, the workstation talks to the DHCP or MacIP server and renews the lease on that IP address. This renewal allows the workstation to keep and use the assigned IP address until the next renewal period.

The term “release” refers to a situation where the workstation is no longer using its assigned IP address or has been shut down. IP addresses can be manually released as well. The IP address goes back into the DHCP or MacIP address pool to be reassigned to another workstation as needed.

Technical note on subnet masking

Note: The IP address supplied by the Router will be a unique number. You may want to replace this number with a number that your ISP supplies if you are configuring the gateway for a static IP address. However, the Router and all devices on the same local network must have the same subnet mask. If you require a different class address, you can edit the IP Mask field to enter the correct address. Refer to the table below.

Number of Devices (other than Router) on Local Network	Largest Possible Ethernet Subnet Mask
1	255.255.255.252
2-5	255.255.255.248 (6)
6-13	255.255.255.240 (14)
14-29	255.255.255.224 (30)
30-61	255.255.255.192
62-125	255.255.255.128
125-259	255.255.255.0

Configuration

This section describes the specific IP address lease, renew, and release mechanisms for both the Mac and PC, with either DHCP or MacIP address serving.

DHCP address serving

Windows 95 workstation:

- The Win95 workstation requests and renews its lease every half hour.
- The Win95 workstation does NOT relinquish its DHCP address lease when the machine is shut down.
- The lease can be manually expired using the WINIPCFG program, a command line program executable from the DOS prompt or from the START:RUN menu on a Windows-based computer.

Windows 3.1 workstation (MSTCP Version 3.11a):

- The Win3.1 workstation requests and renews its lease every half hour.
- The Win3.1 workstation does NOT relinquish its DHCP address lease when the user exits Windows and goes to DOS.
- The lease can be manually expired by typing IPCONFIG/RELEASE from a DOS window within Windows or from the DOS prompt.

Macintosh workstation (Open Transport Version 1.1 or later):

- The Mac workstation requests and renews its lease every half hour.
- The Mac workstation relinquishes its address upon shutdown in all but one case. If the TCP/IP control panel is set to initialize at startup, and no IP services are used or the TCP/IP control panel is not opened, the DHCP address will NOT be relinquished upon shutdown. However, if the TCP/IP control panel is opened or if an IP application is used, the Mac WILL relinquish the lease upon shutdown.
- If the TCP/IP control panel is set to acquire an address only when needed (therefore a TCP/IP application must have been launched to obtain a lease) the Mac WILL relinquish its lease upon shutdown every time.

Netopia Firmware Version 8.4 DHCP server characteristics

- The Netopia Firmware Version 8.4 ignores any lease-time associated with a DHCP request and automatically issues the DHCP address lease for one hour.
- The number of devices a Router can serve DHCP to is 512. This is imposed by global limits on the size of the address serving database, which is shared by all address serving functions active in the gateway.
- The Router releases the DHCP address back to the available DHCP address pool exactly one hour after the last-heard lease request. Some other DHCP implementations may hold on to the lease for an additional time after the lease expired to act as a buffer for variances in clocks between the client and server.

MacIP serving

Macintosh workstation (MacTCP or Open Transport):

Once the Mac workstation requests and receives a valid address, the Router actively checks for the workstation's existence once every minute.

- For a dynamic address, the Router releases the address back to the address pool after it has lost contact with the Mac workstation for over 2 minutes.
- For a static address, the Router releases the address back to the address pool after it has lost contact with the Mac workstation for over 20 minutes.

Netopia Firmware Version 8.4 MacIP server characteristics

The Mac workstation uses ATP to both request and receive an address from the Router's MacIP server. Once acquired, NBP confirm packets will be sent out every minute from the Router to the Mac workstation.

Manually distributing IP addresses

If you choose to manually distribute IP addresses, you must enter each computer's address into its TCP/IP stack software. Once you manually issue an address to a computer, it possesses that address until you manually remove it. That's why manually distributed addresses are called static addresses.

Static addresses are useful in cases when you want to make sure that a host on your network cannot have its address taken away by the address server. Appropriate candidates for a static address include a network administrator's computer, a computer dedicated to communicating with the Internet, and gateways.

Using address serving

The Router provides three ways to serve IP addresses to computers on a network. The first, Dynamic Host Configuration Protocol (DHCP), is supported by PCs with Microsoft Windows and a TCP/IP stack. Macintosh computers using Open Transport and computers using the UNIX operating system may also be able to use DHCP. The second way, MacIP, is for Macintosh computers. The third way, called Serve Dynamic WAN Clients (IPCP), is used to fulfill WAN client requirements.

The Router can use both DHCP and MacIP. Whether you use one or both depends on your particular networking environment. If that environment includes both PCs and Macintosh computers that do not use Open Transport, you need to use both DHCP and MacIP to distribute IP addresses to all of your computers.

Serve dynamic WAN clients

The third method, used to fulfill WAN client requirements, is called Serve Dynamic WAN Clients. The correct term or protocol is a subset of the PPP suite call IPCP. Originally, this would apply only to switched WAN interface gateways, and not to leased line gateways. However, a new feature can give you Asynchronous PPP dial-in support on the Auxiliary port on any gateway including leased line Netopia gateways.

In any situation where a device is dialing into a Netopia gateway, the gateway may need to be configured to serve IP via the WAN interface. This is only a requirement if the calling device has not been configured locally to know what its address(es) are. So when a client, dialing into a Netopia gateway's WAN interface, is expecting addresses to be served by the answering gateway, you must set the answering Netopia gateway to serve IP via its WAN interface.

You can do this in either of two ways:

- use the Serve Dynamic WAN Clients option in the Address Serving Setup screen.

Enabling Serve Dynamic WAN Clients only allows you to specify a pool of addresses from which the dial-in client may get an IP address. It does not allow static addressing.

If you want to serve addresses dynamically, use Serve Dynamic WAN Clients.

- define the address that you want to serve in the Connection Profile's IP Setup screen.

This method requires a static value to be used. Thus any user dialing in can obtain the same IP address for every connection to the profile.

If you want to serve addresses statically, define the address in the Connection Profile.

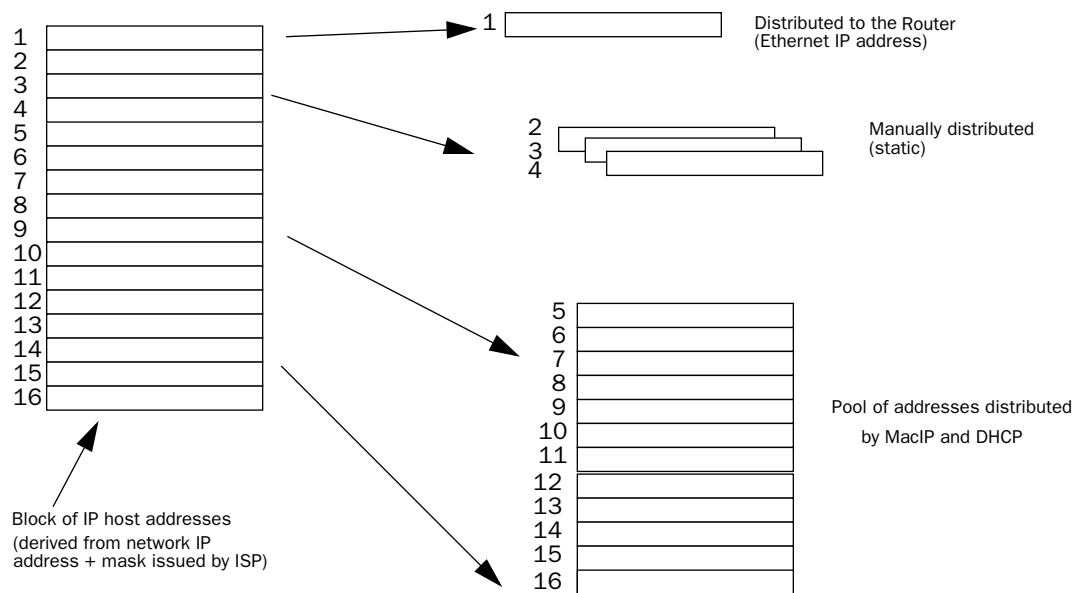
Notes:

- The addresses that are to be served cannot be used elsewhere. For example you wouldn't want to define a static address in a Connection Profile to be served via the WAN that is already defined in the DHCP pool of addresses.
- In order to work correctly, you must define a host or node address in the IP Profile Parameters of the Connection Profile.

This is accomplished by specifying the IP address that is to be statically served via the WAN, and then by entering a mask value of 255.255.255.255.

Tips and rules for distributing IP addresses

- Before you allocate IP addresses using DHCP and MacIP, consider whether you need to set aside any static addresses.
- Note any planned and currently used static addresses before you use DHCP and MacIP.
- Avoid fragmenting your block of IP addresses. For example, try to use a continuous range for the static addresses you choose.



The figure above shows an example of a block of IP addresses being distributed correctly.

The example follows these rules:

- An IP address must not be used as a static address if it is also in a range of addresses being distributed by DHCP or MacIP.
- A single IP address range is used by all the address-served clients. These include DHCP, BootP, MacIP, and WAN clients, even though BootP and static MacIP clients might not be considered served.
- The address range specified for address-served clients cannot wrap around from the end of the total available range back to the beginning. See below for a further explanation and an example.
- The network address issued by an ISP cannot be used as a host address.

A DHCP example

Suppose, for example, that your ISP gave your network the IP address 199.1.1.32 and a 4-bit subnet mask. Address 199.1.1.32 is reserved as the network address. Address 199.1.1.47 is reserved as the broadcast address. This leaves 14 addresses to allocate, from 199.1.1.33 through 199.1.1.46. If you want to allocate a sub-block of 10 addresses using DHCP, enter “10” in the DHCP Setup screen’s **Number of Addresses to Allocate** item. Then, in the same screen’s **First Address** item, enter the first address in the sub-block to allocate so that all 10 addresses are within your original block. You could enter 199.1.1.33, or 199.1.1.37, or any address between them. Note that if you entered 199.1.1.42 as the first address, network routing errors would probably result because you would be using a range with addresses that do not belong to your network (199.1.1.49, 199.1.1.50, and 199.1.1.51). The DHCP server would not initialize if set incorrectly.

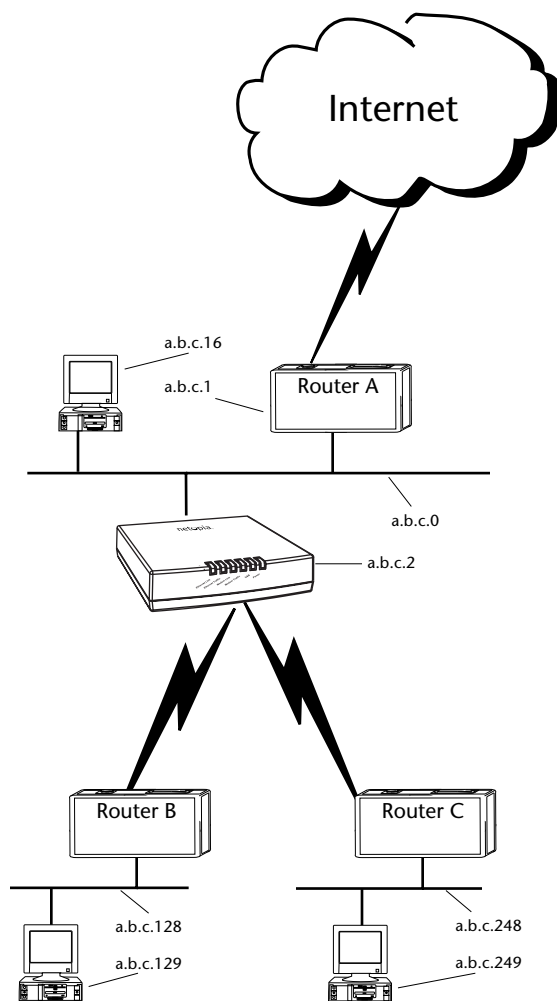
Nested IP Subnets

Under certain circumstances, you may want to create remote subnets from the limited number of IP addresses issued by your ISP or other authority. You can do this using connection profiles. These subnets can be nested within the range of IP addresses available to your network.

For example, suppose that you obtain the Class C network address a.b.c.0 to be distributed among three networks. This network address can be used on your main network, while portions of it can be subnetted to the two remaining networks.

Note: The IP address a.b.c.0 has letters in place of the first three numbers to generalize it for this example.

The figure shows a possible network configuration following this scheme. The main network is set up with the Class C address a.b.c.0, and contains Router A (which could be a Router), a Router, and a number of other hosts. Router A maintains a link to the Internet and can be used as the default gateway.



Routers B and C (which could also be Routers) serve the two remote networks that are subnets of a.b.c.0. The subnetting is accomplished by configuring the Router with connection profiles for Routers B and C (see the following table).

Connection profile	Remote IP address	Remote IP mask	Bits available for host address
For Router B	a.b.c.128	255.255.255.192	7
For Router C	a.b.c.248	255.255.255.248	3

The Router’s connection profiles for Routers B and C create entries in its IP routing table. One entry points to the subnet a.b.c.128, while a second entry points to the subnet a.b.c.248. The IP routing table might look similar to the following:

IP Routing Table				
Network	Address-Subnet Mask	via Gateway	Port	Type
-----SCROLL UP-----				
0.0.0.0	0.0.0.0	a.b.c.1	--	Other
127.0.0.1	255.255.255.255	127.0.0.1	Loopback	Local
a.b.c.128	255.255.255.192	a.b.c.128	WAN	Local
a.b.c.248	255.255.255.248	a.b.c.248	WAN	Local
-----SCROLL DOWN-----				
UPDATE				

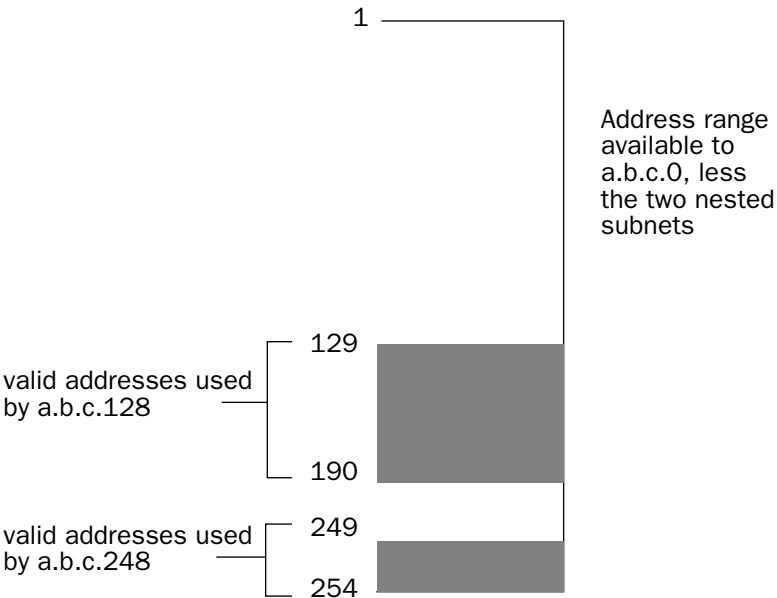
Let’s see how a packet from the Internet gets routed to the host with IP address a.b.c.249, which is served by Router C. The packet first arrives at Router A, which delivers it to its local network (a.b.c.0). The packet is then received by the Router, which examines its destination IP address.

The Router compares the packet’s destination IP address with the routes in its IP routing table. It begins with the route at the bottom of the list and works up until there’s a match or the route to the default gateway is reached.

When a.b.c.249 is masked by the first route’s subnet mask, it yields a.b.c.248, which matches the network address in the route. The Router uses the connection profile associated with the route to connect to Router C, and then forwards the packet. Router C delivers the packet to the host on its local network.

B-14 Firmware User Guide

The following diagram illustrates the IP address space taken up by the two remote IP subnets. You can see from the diagram why the term nested is appropriate for describing these subnets.



Broadcasts

As mentioned earlier, binary IP host or subnet addresses composed entirely of ones or zeros are reserved for broadcasting. A broadcast packet is a packet that is to be delivered to every host on the network if both the host address and the subnet address are all ones or all zeros, or to every host on the subnetwork if the host address is all ones or all zeros but the subnet address is a combination of zeros and ones. Instead of making many copies of the packet, individually addressed to different hosts, all the host machines know to pay attention to broadcast packets, as well as to packets addressed to their specific individual host addresses. Depending on the age and type of IP equipment you use, broadcasts will be addressed using either all zeros or all ones, but not both. If your network requires zeros broadcasting, you must configure this through SNMP.

Packet header types

As previously mentioned, IP works with other protocols to allow communication over IP networks. When IP is used on an Ethernet network, IP works with the Ethernet or 802.3 framing standards, among other protocols. These two protocols specify two different ways to organize the very first signals in the sequence of electrical signals that make up an IP packet travelling over Ethernet. By default, the Router uses Ethernet packet headers for IP traffic. If your network requires 802.3 IP framing, you must configure this through SNMP.

Appendix C

Binary Conversion Table

This table is provided to help you choose subnet numbers and host numbers for IP and MacIP networks that use subnetting for IP addresses.

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
0	0	32	100000	64	1000000	96	1100000
1	1	33	1000001	65	1000001	97	1100001
2	10	34	100010	66	1000010	98	1100010
3	11	35	100011	67	1000011	99	1100011
4	100	36	100100	68	1000100	100	1100100
5	101	37	100101	69	1000101	101	1100101
6	110	38	100110	70	1000110	102	1100110
7	111	39	100111	71	1000111	103	1100111
8	1000	40	101000	72	1001000	104	1101000
9	1001	41	101001	73	1001001	105	1101001
10	1010	42	101010	74	1001010	106	1101010
11	1011	43	101011	75	1001011	107	1101011
12	1100	44	101100	76	1001100	108	1101100
13	1101	45	101101	77	1001101	109	1101101
14	1110	46	101110	78	1001110	110	1101110
15	1111	47	101111	79	1001111	111	1101111
16	10000	48	110000	80	1010000	112	1110000
17	10001	49	110001	81	1010001	113	1110001
18	10010	50	110010	82	1010010	114	1110010
19	10011	51	110011	83	1010011	115	1110011
20	10100	52	110100	84	1010100	116	1110100
21	10101	53	110101	85	1010101	117	1110101
22	10110	54	110110	86	1010110	118	1110110
23	10111	55	110111	87	1010111	119	1110111
24	11000	56	111000	88	1011000	120	1111000
25	11001	57	111001	89	1011001	121	1111001
26	11010	58	111010	90	1011010	122	1111010
27	11011	59	111011	91	1011011	123	1111011
28	11100	60	111100	92	1011100	124	1111100
29	11101	61	111101	93	1011101	125	1111101

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
30	11110	62	111110	94	1011110	126	1111110
31	11111	63	111111	95	1011111	127	1111111

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
128	10000000	160	10100000	192	11000000	224	11100000
129	10000001	161	10100001	193	11000001	225	11100001
130	10000010	162	10100010	194	11000010	226	11100010
131	10000011	163	10100011	195	11000011	227	11100011
132	10000100	164	10100100	196	11000100	228	11100100
133	10000101	165	10100101	197	11000101	229	11100101
134	10000110	166	10100110	198	11000110	230	11100110
135	10000111	167	10100111	199	11000111	231	11100111
136	10001000	168	10101000	200	11001000	232	11101000
137	10001001	169	10101001	201	11001001	233	11101001
138	10001010	170	10101010	202	11001010	234	11101010
139	10001011	171	10101011	203	11001011	235	11101011
140	10001100	172	10101100	204	11001100	236	11101100
141	10001101	173	10101101	205	11001101	237	11101101
142	10001110	174	10101110	206	11001110	238	11101110
143	10001111	175	10101111	207	11001111	239	11101111
144	10010000	176	10110000	208	11010000	240	11110000
145	10010001	177	10110001	209	11010001	241	11110001
146	10010010	178	10110010	210	11010010	242	11110010
147	10010011	179	10110011	211	11010011	243	11110011
148	10010100	180	10110100	212	11010100	244	11110100
149	10010101	181	10110101	213	11010101	245	11110101
150	10010110	182	10110110	214	11010110	246	11110110
151	10010111	183	10110111	215	11010111	247	11110111
152	10011000	184	10111000	216	11011000	248	11111000
153	10011001	185	10111001	217	11011001	249	11111001
154	10011010	186	10111010	218	11011010	250	11111010
155	10011011	187	10111011	219	11011011	251	11111011
156	10011100	188	10111100	220	11011100	252	11111100
157	10011101	189	10111101	221	11011101	253	11111101
158	10011110	190	10111110	222	11011110	254	11111110

Decimal	Binary	Decimal	Binary	Decimal	Binary	Decimal	Binary
159	10011111	191	10111111	223	11011111	255	11111111

Appendix D

Technical Specifications and Safety Information

Description

Dimensions: 13.5 cm (w) x 13.5 cm (d) x 3.5 cm (h); 5.25" (w) x 5.25" (d) x 1.5" (h)

Communications interfaces: The Netopia 3300 Series Routers have an RJ-11 jack for DSL line connections or an RJ-45 jack for Ethernet WAN line connections and 1 or 4-port 10/100Base-T Ethernet switch for your LAN connections. Some models have a USB port that can be used to connect to your PC; in some cases, the USB port also serves as the power source. Some models contain an 802.11b wireless LAN transmitter.

Power requirements

- 12 VDC input
- 1.0 amps
- **USB-powered models only:** For Use with Listed I.T.E. Only

Environment

Operating temperature: 0° to +40° C

Storage temperature: 0° to +70° C

Relative storage humidity: 20 to 80% noncondensing

Software and protocols

Software media: Software preloaded on internal flash memory; field upgrades done via download to internal flash memory via TFTP.

Routing: TCP/IP Internet Protocol Suite, RIP

WAN support: PPPoE, DHCP, static IP address

Security: PAP, UI password security

Management/configuration methods: Telnet, SNMP, Command Line Interface (CLI)

Diagnostics: Ping, event logging, routing table displays, traceroute, statistics counters

Agency approvals

North America

Safety Approvals:

- United States – UL 60950 Third Edition
- Canada – CSA: CAN/CSA-C22.2 No. 60950-00

EMC:

- United States – FCC Part 15 Class B
- Canada – ICES-003

Telecom:

- United States – FCC Part 68
- Canada – CS-03

International

Safety Approvals:

- Low Voltage (European directive) 73/23
- EN60950 (Europe)

EMI Compatibility:

- 89/336/EEC (European directive)
- EN55022:1994 CISPR22 Class B
- EN300 386 V1.2.1 (non-wireless products)
- EN 301-489 (wireless products)

Regulatory notices

European Community. This Netopia product conforms to the European Community CE Mark standard for the design and manufacturing of information technology equipment. This standard covers a broad area of product design, including RF emissions and immunity from electrical disturbances.

The Netopia Firmware Version 8.4 complies with the following EU directives:

- Low Voltage, 73/23/EEC
- EMC Compatibility, 89/336/EEC, conforming to EN 55 022

Manufacturer's Declaration of Conformance

Note: Warnings:

This is a Class B product. In a domestic environment this product may cause radio interference, in which case the user may be required to take adequate measures. Adequate measures include increasing the physical distance between this product and other electrical devices.

Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

United States. Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Service requirements. In the event of equipment malfunction, all repairs should be performed by our Company or an authorized agent. It is the responsibility of users requiring service to report the need for service to our Company or to one of our authorized agents. Service can be obtained at Netopia, Inc., 6001 Shellmound Street, Emeryville, California, 94608. Telephone: 510-597-5400.

Note: Important

This product was tested for FCC compliance under conditions that included the use of shielded cables and connectors between system components. Changes or modifications to this product not authorized by the manufacturer could void your authority to operate the equipment.

Canada. This Class B digital apparatus meets all requirements of the Canadian Interference -Causing Equipment Regulations.

Cet appareil numérique de la classe B respecte toutes les exigences du Règlement sur le matériel brouilleur du Canada.

Declaration for Canadian users

NOTICE: The Canadian Industry Canada label identifies certified equipment. This certification means that the equipment meets certain telecommunications network protective, operation, and safety requirements. The Department does not guarantee the equipment will operate to the user's satisfaction.

Before installing this equipment, users should ensure that it is permissible to be connected to the facilities of the local telecommunications company. The equipment must also be installed using an acceptable method of connection. In some cases, the company's inside wiring associated with a single line individual service may be extended by means of a certified connector assembly (telephone extension cord). The customer should be aware that compliance with the above conditions may not prevent degradation of service in some situations.

Repairs to the certified equipment should be made by an authorized Canadian maintenance facility designated by the supplier. Any repairs or alterations made by the user to this equipment, or equipment malfunctions, may give the telecommunications company cause to request the user to disconnect the equipment.

Users should ensure for their own protection that the electrical ground connections of the power utility, telephone lines, and internal metallic water pipe system, if present, are connected together. This precaution may be particularly important in rural areas.

Caution

Users should not attempt to make such connections themselves, but should contact the appropriate electric inspection authority, or electrician, as appropriate.

The Ringer Equivalence Number (REN) assigned to each terminal device provides an indication of the maximum number of terminals allowed to be connected to a telephone interface. The termination on an interface may consist of any combination of devices subject only to the requirement that the sum of the Ringer Equivalence Numbers of all the devices does not exceed 5.

Important Safety Instructions

Australian Safety Information

The following safety information is provided in conformance with Australian safety requirements:

Caution

DO NOT USE BEFORE READING THE INSTRUCTIONS: Do not connect the Ethernet ports to a carrier or carriage service provider's telecommunications network or facility unless: a) you have the written consent of the network or facility manager, or b) the connection is in accordance with a connection permit or connection rules.

Connection of the Ethernet ports may cause a hazard or damage to the telecommunication network or facility, or persons, with consequential liability for substantial compensation.

Caution

- Depending on the power supply provided with the product, either the direct plug-in power supply blades, power supply cord plug or the appliance coupler serves as the mains power disconnect. It is important that the direct plug-in power supply, socket-outlet or appliance coupler be located so it is readily accessible.
CAUTION (North America Only): For use only with a CSA Certified or UL Listed Limited Power Source or Class 2 power supply, rated 12Vdc, 1.5A.
- (Sweden)** Apparaten skall anslutas till jordat uttag när den ansluts till ett nätverk
- (Norway)** Apparatet må kun tilkoples jordet stikkontakt.

- **USB-powered models:** For Use with Listed I.T.E. Only.

Telecommunication installation cautions

- Never install telephone wiring during a lightning storm.
- Never install telephone jacks in wet locations unless the jack is specifically designed for wet locations.
- Never touch uninsulated telephone wires or terminals unless the telephone line has been disconnected at the network interface.
- Use caution when installing or modifying telephone lines.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightning.
- Do not use the telephone to report a gas leak in the vicinity of the leak.

FCC Part 68 Information

FCC Requirements

1. The Federal Communications Commission (FCC) has established Rules which permit this device to be directly connected to the telephone network. Standardized jacks are used for these connections. This equipment should not be used on party lines or coin phones.
2. If this device is malfunctioning, it may also be causing harm to the telephone network; this device should be disconnected until the source of the problem can be determined and until repair has been made. If this is not done, the telephone company may temporarily disconnect service.
3. The telephone company may make changes in its technical operations and procedures; if such changes affect the compatibility or use of this device, the telephone company is required to give adequate notice of the changes. You will be advised of your right to file a complaint with the FCC.
4. If the telephone company requests information on what equipment is connected to their lines, inform them of:
 - a. The telephone number to which this unit is connected.
 - b. The ringer equivalence number. [0.XB]
 - c. The USOC jack required. [RJ11C]
 - d. The FCC Registration Number. [XXXUSA-XXXXX-XX-E]

Items (b) and (d) are indicated on the label. The Ringer Equivalence Number (REN) is used to determine how many devices can be connected to your telephone line. In most areas, the sum of the REN's of all devices on any one line should not exceed five (5.0). If too many devices are attached, they may not ring properly.

FCC Statements

a) This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US:AAAEQ##TXXXX. If requested, this number must be provided to the telephone company.

- b) List all applicable certification jack Universal Service Order Codes (“USOC”) for the equipment: RJ11.
- c) A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.
- d) The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. In most but not all areas, the sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. For products approved after July 23, 2002, the REN for this product is part of the product identifier that has the format US:AAAEQ##TXXXX. The digits represented by ## are the REN without a decimal point (e.g., 03 is a REN of 0.3). For earlier products, the REN is separately shown on the label.
- e) If this equipment, the Netopia 3300 Series router, causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn’t practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.
- f) The telephone company may make changes in its facilities, equipment, operations or procedures that could affect the operation of the equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.
- g) If trouble is experienced with this equipment, the Netopia 3300 Series router, for repair or warranty information, please contact:
- Netopia Technical Support
510-597-5400
www.netopia.com.
- If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is resolved.
- h) This equipment not intended to be repaired by the end user. In case of any problems, please refer to the troubleshooting section of the Product User Manual before calling Netopia Technical Support.
- i) Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information.
- j) If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this Netopia 3300 Series router does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or qualified installer.

RF Exposure Statement:

Note: Installation of the wireless models must maintain at least 20 cm between the wireless router and any body part of the user to be in compliance with FCC RF exposure guidelines.

Electrical Safety Advisory

Telephone companies report that electrical surges, typically lightning transients, are very destructive to customer terminal equipment connected to AC power sources. This has been identified as a major nationwide problem. Therefore it is advised that this equipment be connected to AC power through the use of a surge arrester or similar protection device.

Index

A

- add static route 6-8
- ADSL Line Configuration 2-4
- advanced configuration
 - features 2-22
- ATMP 4-17
 - tunnel options 4-15

B

- backup default gateway 7-14
- backup, line 7-1
- basic firewall 9-30
- BootP 6-17
 - clients 6-23
- broadcasts B-14

C

- change static route 6-9
- community strings 8-12
- configuration
 - troubleshooting
 - PC A-1
- configuration files
 - downloading with TFTP 10-7
 - uploading with TFTP 10-8
- Configuration Management 9-42
- configuring
 - with console-based management 1-2, 2-1
- configuring terminal emulation software 1-4
- Connection profiles 2-9
- console-based management

- configuring with 1-2, 2-1
- Constant Bit Rate (CBR) 2-6

D

- D. port 9-21
- Data Encryption Standard (DES) 4-17
- date and time
 - setting 2-29
- dead peer detection 5-12
- delayed configuration 2-14
- delete static route 6-9
- DES 4-3, 4-7, 5-1
- designing a new filter set 9-23
- DHCP
 - defined B-8
- DHCP Lease 6-18
- DHCP NetBIOS options 6-21
- DHCP Relay Agent 6-28
- display static routes 6-7
- distributing IP addresses B-5
- downloading configuration files 10-7
 - with TFTP 10-7
- Dynamic Host Configuration Protocol (DHCP) 6-17
- Dynamic Host Configuration Protocol, *see DHCP*
- Dynamic WAN 6-17

E

- Easy Setup
 - navigating 1-4
- encryption 4-2, 4-7, 4-17, 5-1
- event history
 - device 8-5
 - WAN 8-5
- Exposed Addresses 2-27

F

filter

- parts 9-19
- parts of 9-19

filter priority 9-18

filter set

- adding 9-25
- display 9-21

filter sets

- adding 9-25
- defined 9-17
- deleting 9-29
- disadvantages 9-23
- sample (Basic Firewall) 9-29
- using 9-24

filtering example #1 9-22

filters

- actions a filter can take 9-18
- adding to a filter set 9-26
- defined 9-17
- deleting 9-29
- disadvantages of 9-23
- input 9-26
- modifying 9-28
- output 9-26
- using 9-23, 9-24
- viewing 9-28

firewall 9-29

firmware files

- updating with TFTP 10-7

FTP sessions 9-32

G

general statistics 8-7

Generic Routing Encapsulation 4-11

GRE 4-11

H

how to reach us A-4

I

IKE 5-1

input filter 3 9-30

input filters 1 and 2 9-30

input filters 4 and 5 9-30

Internet addresses, *see IP addresses*

Internet Key Exchange 5-1

Internet Key Exchange (IKE) 4-7, 5-1

Internet Protocol (IP) 6-1

IP address serving 6-17

IP addresses B-1

- about B-1
- distributing B-5
- distribution rules B-10
- static B-8

IP setup 6-2

IP trap receivers

- deleting 8-13
- modifying 8-13
- setting 8-13
- viewing 8-13

IPsec 4-2, 4-7, 5-1

L

L2TP 4-8

latency 2-20, 9-33

Layer 2 Tunnelling Protocol 4-8

LED status 8-3

LEDs 8-3

line backup 7-1

- backup IP gateway 7-16
- connection profiles 7-2

- management and statistics 7-17
- scheduled connections 7-12
- WAN configuration 7-8

M

- MIBs supported 8-10
- model numbers 1-3
- MPPE 4-17
- MS-CHAPv2 4-18
- Multicast Forwarding 6-33
- multiple subnets 6-4

N

- NAT
 - adding server lists 3-15
 - defined 6-1
 - Easy Setup Profile 3-6
 - IP profile parameters 3-21
 - IP setup 3-7
 - map lists 3-8
 - modifying map lists 3-12
 - outside ranges 3-8
 - server lists 3-8
- navigating
 - Easy Setup 1-4
- NCSA Telnet 1-4
- nested IP subnets B-11
- NetBIOS 6-21
- NetBIOS scope 6-22
- Netopia
 - distributing IP addresses 6-17, B-5
 - models 1-3
 - monitoring 8-1
 - security 9-1
 - system utilities and diagnostics 10-1
- Network Address Translation

- see NAT 6-1

- network problems A-2
- network status overview 8-1

O

- output filter 1 9-31

P

- packet
 - header B-14
- PAT (Port Address Translation) 3-2
- permanent virtual circuit 2-4
- ping 10-2
- ping test, configuring and initiating 10-2
- policy-based routing 9-32
- port number
 - comparisons 9-20
- port numbers 9-19
- PPTP 4-17
 - tunnel options 4-4
- priority queuing 2-20
- PVC 2-4

Q

- quality of service 2-20, 9-33
- Quick View 8-1

R

- restarting the system 10-8
- restricting telnet access 9-16
- RFC-1483 Transparent Bridging 2-37
- RIP 2-3, 2-13
- RIP-2 MD5 Authentication 6-10
- router to serve IP addresses to hosts 6-1
- routing tables
 - IP 6-6, 8-7

S

scheduled connections 2-15

- adding 2-17

- deleting 2-20

- modifying 2-20

- once-only 2-19

- viewing 2-16

- weekly 2-18

security

- filters 9-17–9-32

- measures to increase 9-1

- telnet 9-16

Security Policy Database (SPD) 5-2

Simple Network Management Protocol,

see SNMP

SNMP

- community strings 8-12

- MIBs supported 8-10

- setup screen 8-11

- traps 8-12

SNMP-V2c 8-10

src. port

- 9-21

SSID (Wireless ID) 2-30

Stateful inspection 2-23

static IP addresses B-8

static route

- rules of installation 6-9

static routes 6-3, 6-6

strong encryption 4-18

subnet masks B-3

subnets B-2–B-5

- multiple 6-4

- nested B-11

subnets and subnet masks B-2

support

- technical A-3

T

technical support A-3

telnet 1-3

- access 9-16

terminal emulation software

- configuring 1-4

TFTP

- defined 10-6

- downloading configuration files 10-7

- updating firmware 10-7

- uploading configuration files 10-8

TFTP, transferring files 10-6

tiered access 9-2

TOS bit 2-21, 9-33

Trivial File Transfer Protocol (TFTP) 10-6

Trivial File Transfer Protocol, *see TFTP*

troubleshooting A-1

- configuration

 - PC A-1

- event histories 8-4

trusted host 9-31

trusted subnet 9-31

tunnel options

- ATMP 4-15

- PPTP 4-4

tunneling 4-2

U

Unspecified Bit Rate (UBR) 2-6

updating firmware

- with TFTP 10-7

updating Netopia's firmware 10-7

- upgrade 1-3
- uploading configuration files 10-8
 - with TFTP 10-8
- utilities and diagnostics 10-1

V

- Variable Bit Rate (VBR) 2-6
- viewing scheduled connections 2-16
- Virtual Private Networks (VPN) 4-1
- VPN 4-1
 - allowing through a firewall 4-24
 - ATMP tunnel options 4-15
 - default answer profile 4-18
 - encryption support 4-17
 - PPTP tunnel options 4-4

W

- WAN
 - event history 8-5
- WAN Ethernet Configuration 2-2
- WAN event history 8-5
- WEP (Wired Equivalent Privacy) 2-32
- Wi-Fi Protected Access 2-31
- Windows NT Domain Name 4-6
- Wireless Configuration 2-30
- Wireless MAC Authentication 2-34
- WPA 2-31

